# Algèbre-III
# Réduction des endomorphismes

Alexis Tchoudjem

Université Lyon I



10 octobre 2011

Dans ce cours $\mathbb{K}$ est un corps qui peut être $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.

# Table des matières

# Chapitre 1

# Un peu de théorie des groupes

## 1.1 Lois de composition

De manière très générale, *faire de l'algèbre* c'est étudier des structures algébriques *c-à-d* des ensembles où sont définies des opérations.

Une *opération*, ou *loi de composition*, sur un ensemble $E$ est une application :

$$E \times E \to E \ .$$

Les éléments de l'ensemble $E$ peuvent être des nombres, des matrices, des fonctions, *etc*

Les ensembles de nombres suivants sont des exemples basiques de structures algébriques. Ils sont munis d'au moins deux opérations, l'addition et la multiplication :

$$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{R}_+ \ .$$

**Remarques :**

— les opérations d'addition et de multiplication ne sont pas définies sur tous les ensembles de nombres. Par exemple le produit de deux nombres irrationnels n'est pas toujours un nombre irrationnel ;

— Le produit vectoriel des vecteurs de $\mathbb{R}^3$ est un exemple de loi de composition mais non le produit scalaire.

Rappelons que le produit vectoriel sur $\mathbb{R}^3$ est défini ainsi :

$$^{\forall} x_i, y_j \in \mathbb{R}, \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \wedge \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} := \begin{pmatrix} x_2y_3 - x_3y_2 \\ x_3y_1 - x_1y_3 \\ x_1y_2 - x_2y_1 \end{pmatrix} \ .$$

**Notations :** Pour une loi de composition sur un ensemble $E$, la notation fonctionnelle n'est pas très pratique. On utilise plutôt une notation qui ressemble à celle utilisée pour la somme ou le produit de nombres. Par exemple, si :

$$p : E \times E \to E \ (a, b) \mapsto p(a, b)$$

est une loi de composition on notera le plus souvent $ab$ (ou parfois $a \times b, a \circ b$ ou $a + b$) le résultat de l'opération $p(a, b)$. Par exemple : $(ab)c = p(p(a, b), c)$.

### 1.1.1 Associativité, commutativité

**Définition 1** *Soit une loi de composition sur un ensemble $E$ notée multiplicativement : $(a, b) \mapsto ab$. On dit que cette loi est associative si :*

$$(ab)c = a(bc)$$

*pour tous $a, b, c \in E$. On dit que cette loi est commutative si :*

$$ab = ba$$

*pour tous $a, b \in E$.*

**Exemples :** les lois d'addition et de multiplications sur les ensembles de nombres $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$ sont associatives et commutatives. La loi d'addition (coordonnée par coordonnée) sur l'ensemble des vecteurs de $\mathbb{R}^n$ est aussi associative et commutative. En revanche, la loi du produit vectoriel sur les vecteurs de $\mathbb{R}^3$ n'est ni associative ni commutative. La loi de multiplication des matrices carrées (réelles ou complexes) est une loi associative.

**Notations :** on note souvent $+$ les lois de composition commutatives.

**Remarque :** Si une loi $(a, b) \mapsto ab$ sur un ensemble $E$ est associative, on définit le produit de $n$ éléments de $E$ par récurrence sur $n$ de la façon suivante :

$$a_1 \ldots a_n := (a_1 \ldots a_{n-1})a_n$$

pour tous $a_1, \ldots a_n \in E$. On a alors :

$$a_1 \ldots a_n = (a_1 \ldots a_i)(a_{i+1} \ldots a_n)$$

pour tout $1 \leq i \leq n$.

**Exemple :** On note $\mathscr{M}_n(\mathbb{R}) := \left\{ \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} : a_{i,j} \in \mathbb{R} \right\}$ l'ensemble des matrices réelles de taille $n \times n$. Si $A = (a_{i,j})_{1 \leq i,j \leq n}, B = (b_{i,j})_{1 \leq i,j \leq n}$

sont des matrices carrées réelles, on pose $AB := (c_{i,j})_{1\leq i,j\leq n}$ où :

$$c_{i,j} = \sum_{k=1}^{n} a_{i,k}b_{k,j} \ .$$

Cette loi est associative, en effet, si $A = (a_{i,j})_{1\leq i,j\leq n}, B = (b_{i,j})_{1\leq i,j\leq n}, C = (c_{i,j})_{1\leq i,j\leq n}$, alors pour tous $i, j$, le $(i, j)-$ième coefficient de $(AB)C$ est le même que le $(i, j)-$ième coefficient de $A(BC)$ :

$$\sum_{1\leq k,l\leq n} a_{i,k}b_{k,l}c_{l,j} \ .$$

### 1.1.2 Identité, éléments inversibles

**Définition 2** *Soit une loi de composition sur un ensemble $E$ :*

$$E \times E \to E \, , (a, b) \mapsto ab \ .$$

*Une identité, ou un élément neutre, pour cette loi est un élément $e \in E$ tel que pour tout $a \in E$ :*

$$ae = ea = a \ .$$

**Proposition 1.1.1** *Si une loi de composition sur un ensemble $E$ a un élément neutre, alors cet élément neutre est unique.*

*Démonstration* : Soient $e, e'$ deux éléments neutres, alors :

$$e = ee' = e' \ .$$

*q.e.d.*

**Exemples :**

— L'élément neutre de l'addition sur l'ensemble des nombres entiers (rationnels, réels, complexes) est 0. — L'élément neutre de l'addition sur l'ensemble des vecteurs de $\mathbb{R}^n$ est le vecteur nul (dont toutes les coordonnées sont 0).

— L'élément neutre de la multiplication sur l'ensemble des nombres entiers (rationnels, réels, complexes) est 1.

— Il n'y a pas délément neutre pour la loi du produit vectoriel sur $\mathbb{R}^3$.

**Notations :** on note souvent 1 le neutre d'une loi de composition notée multiplicativement et 0 le neutre d'une loi de composition notée additivement.

**Exemple :** soit $F$ un ensemble. On note $F^F$ l'ensemble des applications de $F$ dans $F$. Sur cet ensemble $F^F$ on choisit la loi de composition des applications $(f, g) \mapsto f \circ g$. Pour cette loi, l'élément neutre est l'application $\mathrm{Id}_F : F \to F \, , x \mapsto x$.

**Exercice 1** *Vérifier que le neutre pour la multiplication des matrices (à coefficients entiers, rationnels, réels ou complexes) $n \times n$ est la matrice :*

$$I_n := \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} .$$

**Définition 3** *Soit $E$ un ensemble muni d'une loi de composition (notée multiplicativement) qui a un élément neutre $e$. Un élément $x \in E$ est inversible s'il existe un élément $y \in E$ tel que :*

$$xy = yx = e$$

*et dans ce cas, on dit que $y$ est un inverse de $x$. Un élément $x \in E$ est inversible à droite , respectivement inversible à gauche, s'il existe un élément $y \in E$ tel que $xy = e$, respectivement $yx = e$.*

**Exercice 2** *Soit $E$ un ensemble. Considérons la loi de composition des applications sur l'ensemble $E^E$. Soit une application $f : E \to E$. Vérifier les équivalences suivantes :*

— *l'application $f$ est injective $\Leftrightarrow$ $f$ est inversible à gauche ;*
— *l'application $f$ est surjective $\Leftrightarrow$ $f$ est inversible à droite ;*
— *l'application $f$ est bijective $\Leftrightarrow$ $f$ est inversible.*

*Si de plus $E$ est fini, alors $f$ est inversible à gauche $\Leftrightarrow$ $f$ est inversible à droite $\Leftrightarrow$ $f$ est inversible.*

**Proposition 1.1.2** *Soit une loi de composition : $E \times E \to E$, $(a, b) \mapsto ab$* **associative** *avec un élément neutre. Si un élément $a$ est inversible, alors il a un unique inverse, que l'on note $a^{-1}$.*

**Notation :** Si la loi est notée additivement, on note plutôt l'inverse de $a$ par $-a$.

**Exercice 3** *Soit une loi de composition : $E \times E \to E$, $(a, b) \mapsto ab$* **associative** *avec un élément neutre. Si un élément $a$ a un inverse à gauche $b$, un inverse à droite $c$, alors $a$ est inversible et $a^{-1} = b = c$ est l'inverse de $a$.*

« L'inversion renverse la multiplication » :

**Proposition 1.1.3** *Soit une loi de composition : $E \times E \to E$, $(a, b) \mapsto ab$* **associative** *avec un élément neutre. Si $a, b$ sont des éléments inversibles, alors le produit $ab$ est aussi inversible et :*

$$(ab)^{-1} = b^{-1}a^{-1}$$

*Démonstration* : On a : $(ab)b^{-1}a^{-1} = aa^{-1} = 1 = b^{-1}a^{-1}ab$. *q.e.d.*

**Remarque :** pour une loi non commutative, on évite la notation $\frac{a}{b}$ car elle ne permet pas de distinguer $ab^{-1}$ de $b^{-1}a$.

**Notation :** Si $E$ est un ensemble muni d'une loi associative, on note $a^n := \underbrace{a...a}_{n\,\text{fois}}$ pour tout $n$ entier $> 0$. S'il existe un élément neutre $e$, on pose $a^0 := e$. Si de plus, l'élément $a$ est inversible, on note $a^{-n} := (a^{-1})^n$. On vérifie alors que $a^{r+s} = a^r a^s$ et $(a^r)^s = a^{rs}$ pour tous entiers $r, s \in \mathbb{Z}$.

## 1.2 Groupes

**Définition 4** *Un groupe est un ensemble muni d'une loi de composition* **associative** *qui a un élément neutre et dont tous les éléments sont inversibles. Si de plus la loi de composition est commutative, on dit que le groupe est abélien .*

**Remarque :** on note souvent avec la même lettre le groupe et l'ensemble de ses éléments.

**Exemples :**

$$(\mathbb{Z}, +) \text{ l'ensemble des nombres entiers muni de l'addition}$$

$$(\mathbb{Q}, +), \text{ l'ensemble des nombres rationnels muni de l'addition}$$

$$\mathbb{Q}^\times, \text{ l'ensemble des nombres rationnels NON NULS muni de la multiplication}$$

$$(\mathbb{R}, +), \text{ l'ensemble des nombres réels muni de l'addition}$$

$$\mathbb{R}^\times, \text{ l'ensemble des nombres réels NON NULS muni de la multiplication}$$

$$(\mathbb{C}, +), \text{ l'ensemble des nombres complexes muni de l'addition}$$

$$\mathbb{C}^\times, \text{ l'ensemble des nombres complexes NON NULS muni de la multiplication}$$

sont des exemples de groupes abéliens.

En revanche, $\mathbb{N}$ n'est pas un groupe pour l'addition.

Le groupe trivial est le singleton $\{0\}$ avec la loi évidente. Notons $P$ l'ensemble des nombres pairs et $I$ l'ensemble des nombres impairs. On munit l'ensemble $\{P, I\}$ de la loi suivante :

| $+$ | $P$ | $I$ |
|---|---|---|
| $P$ | $P$ | $I$ |
| $I$ | $I$ | $P$ |

*i.e.* : $P + P := P, P + I := I$, *etc.*

On obtient ainsi un groupe abélien à deux éléments. C'est le groupe $\mathbb{Z}/2\mathbb{Z}$.

**Un exemple non commutatif :** Si $\alpha \in \mathbb{R}$, on note $s_\alpha$ la réflexion orthogonale par rapport à la droite du plan qui passe par 0 et qui fait un angle $\alpha$ avec l'axe des abscisses et on note $r_\alpha$ la rotation de centre 0 et d'angle $\alpha$. Alors l'ensemble :

$$O_2 := \{s_\alpha, r_\beta \ : \ \alpha, \beta \in \mathbb{R}\}$$

muni de la loi de composition des applications est un groupe non abélien. En effet, $r_\beta s_\alpha = s_{\alpha+\beta/2}$ et $s_\alpha r_\beta = s_{\alpha-\beta/2}$.

**Exercice 4** *L'ensemble des applications affines non constantes de* $\mathbb{R}$ *dans* $\mathbb{R}$, $x \mapsto ax + b$, $a, b \in \mathbb{R}$, $a \neq 0$, *est un groupe non abélien pour la loi de composition des applications.*

**Proposition 1.2.1 (Loi de simplification)** *Soient* $a, b, c$ *trois éléments d'un groupe* $G$. *Si* $ab = ac$, *alors* $b = c$. *Si* $ba = ca$, *alors* $b = c$.

*Démonstration :* Il suffit de multiplier à gauche ou à droite par $a^{-1}$. *q.e.d.*

**Exercice 5** *Si* $E$ *est un ensemble, l'ensemble des applications bijectives de* $E$ *dans* $E$ *muni de la loi de composition des applications est un groupe.*

**Définition 5 (Groupe symétrique)** *On appelle groupe symétrique d'indice* $n$ *le groupe des bijections de l'ensemble* $\{1, ..., n\}$. *On le note* $S_n$. *Ses éléments sont aussi appelés les permutations de l'ensemble* $\{1, ..., n\}$.

**Exercice 6** *Vérifier que* $S_n$ *est un groupe fini ayant* $n!$ *éléments.*

Si $G$ est un groupe fini, on appelle *ordre* son cardinal.

**Exemples :** — Si $n = 2$, on note $e$ l'identité de $\{1, 2\}$ et $\tau$ l'application $\tau : 1 \mapsto 2,\ 2 \mapsto 1$. On a :

$$S_2 = \{e, \tau\},\ \tau^2 = e\ .$$

— Si $n = 3$, on note $e$ l'identité de $\{1, 2, 3\}$, $s_1$ la permutation $1 \mapsto 2,\ 2 \mapsto 1,\ 3 \mapsto 3$, $s_2$ la permutation $1 \mapsto 1,\ 2 \mapsto 3,\ 3 \mapsto 2$. On a :

$$s_1 s_2 \neq s_2 s_1$$

($S_3$ est le plus petit groupe non abélien)

$$s_1^2 = s_2^2 = e, (s_1 s_2)^3 = e, s_1 s_2 s_1 = s_2 s_1 s_2$$

$$S_3 = \{e, s_1, s_2, s_1s_2, s_2s_1, s_1s_2s_1\} \ .$$

— Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on note dét $A := ad - bc$. L'ensemble $G$ des matrices $A$ $2\times 2$ complexes de déterminant dét $A \neq 0$, muni de la loi de multiplication des matrices est un groupe.

En effet, si $A, B$ sont des matrices $2 \times 2$ complexes telles que dét $A \neq 0$, dét $B \neq 0$, alors dét $(AB) =$ dét $A$dét $B \neq 0$. Donc le produit des matrices est bien une loi de composition sur $G$. Cette loi est associative car la multiplication des matrices l'est. L'élément $I_2$ est l'élément neutre. Et enfin toute matrice

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$$

est inversible d'inverse :

$$A^{-1} = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} \ .$$

Ce groupe est noté $\mathrm{GL}_2(\mathbb{C})$. Si on remplace $\mathbb{C}$ par $\mathbb{R}$, on obtient aussi un groupe noté $\mathrm{GL}_2(\mathbb{R})$.

## 1.3 Sous-groupes

**Définition 6** *Soit $G$ un groupe. Une partie $H$ de $G$ est un sous-groupe si les trois conditions suivantes sont vérifiées :*
*i) $1 \in H$ ;*
*ii) $H$ est stable par multiplication ;*
*iii) $H$ est stable par passage à l'inverse.*

**Remarque :** Si $H$ est un sous-groupe de $G$, alors la loi de composition de $G$ induit une loi de composition sur $H$ (exo) et pour cette loi, $H$ est un groupe. En particulier, pour montrer qu'un ensemble muni d'une loi de composition est un groupe il suffit de montrer que c'est un sous-groupe (ce qui évite d'avoir à vérifier la propriété d'associativité par exemple).

**Exemples :**

— Un groupe $G$, de neutre $e$, a toujours comme sous-groupe $G$ et $\{e\}$ ;

— Si $k$ est un entier, l'ensemble des multiples de $k$, noté $k\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ ;

— l'ensemble des nombres complexes de module 1 est un sous-groupe de $\mathbb{C}^\times$ ;

— l'ensemble $\boldsymbol{\mu}_n$ des racines complexes $n-$ièmes de l'unité est un sous-groupe fini de $\mathbb{C}^\times$ ;

— l'ensemble des rotations du plan de centre 0 est un sous-groupe du groupe $O_2$ ;

— l'ensemble des matrices triangulaires supérieures $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, $a, b, d \in \mathbb{C}$, $a, d \neq 0$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ ;

— l'ensemble des matrices $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ ;

— Soient

$$I := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \; J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \; K := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

l'ensemble $\{\pm I_2, \pm I, \pm J, \pm K\}$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ d'ordre 8 noté $Q_8$.

**Notation :** $H \leq G$ signifie « $H$ est un sous-groupe de $G$ ».

**Les sous-groupes de $\mathbb{Z}$**

**Proposition 1.3.1** *Soit $H$ un sous-groupe de $\mathbb{Z}$ (pour l'addition). Alors, $H = k\mathbb{Z}$ pour un unique entier $k \geq 0$.*

*Démonstration :* Soit $k$ le plus petit entier $> 0$ appartenant à $H$. il suffit de faire une division euclidienne ! *q.e.d.*

Soient $a, b$ des entiers non tous deux nuls . L'ensemble :

$$a\mathbb{Z} + b\mathbb{Z} := \{ar + bs \; : \; r, s \in \mathbb{Z}\}$$

est un sous-groupe non nul de $\mathbb{Z}$. Soit $d$ l'unique entier $> 0$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. On dit que $d$ est le *pgcd* de $a, b$.

# 1.4 Groupes cycliques

## 1.4.1 Les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$

Soit $n$ un entier. On pose $\overline{x} := x + n\mathbb{Z} := \{x + nr \; : \; r \in \mathbb{Z}\}$ pour tout entier $x$. On appelle classes modulo $n$ ces ensembles $\overline{x}$.

Par exemple, si $n = 2$ alors $\overline{0}$ est l'ensemble des nombres pairs et $\overline{1}$ est l'ensemble des nombres impairs.

**Proposition 1.4.1** *Pour deux entiers $x, y$, on a l'équivalence :*

$$x + n\mathbb{Z} = y + n\mathbb{Z} \Leftrightarrow n | x - y \ .$$

**Notation :** pour tous entiers $x, y$, si $x + n\mathbb{Z} = y + n\mathbb{Z}$, on note :

$$x = y \bmod n \ .$$

Bien entendu, on a pour tous entiers $x, y, z$ :

$$x = x \bmod n$$

$$x = y \bmod n \Rightarrow y = x \bmod n \, ,$$

$$x = y \bmod n \text{ et } y = z \bmod n \Rightarrow x = z \bmod n$$

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des $x + n\mathbb{Z}$, $x \in \mathbb{Z}$. C'est l'ensemble des classes modulo $n$.

**Proposition 1.4.2** *Il y a exactement $n$ classes modulo $n$ ; ce sont :*

$$\overline{0}, ..., \overline{n-1} \ .$$

*Démonstration* : Soit $x$ un entier. Alors $\overline{x} = \overline{r}$ où $r$ est le reste de la division euclidienne de $x$ par $n$. *q.e.d.*

On définit une addition sur $\mathbb{Z}/n\mathbb{Z}$ par :

$$(x + n\mathbb{Z}) + (y + n\mathbb{Z}) := (x + y) + n\mathbb{Z} \ .$$

Cette addition est bien définie. En effet, on a :

**Proposition 1.4.3** *Si $x = x' \bmod n$ et $y = y' \bmod n$, alors $x + y = x' + y' \bmod n$.*

**Exemple :** voici la table d'addition du groupe $\mathbb{Z}/3\mathbb{Z}$ :

| + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

.

**Remarque :** on peut aussi définir une multiplication sur $\mathbb{Z}/n\mathbb{Z}$.
Soit $G$ un groupe de neutre 1. Si $x \in G$, on note :

$$\langle x \rangle := \{...x^{-2}, x,^{-1} 1, x, x^2, ...\}$$

$$= \{x^m \ : \ m \in \mathbb{Z}\} \ .$$

C'est le plus petit sous-groupe de $G$ contenant $x$ (*exo*) . On appelle ce sous-groupe le sous-groupe engendré par $x$.

**Lemme 1.4.4** *Soit $G$ un groupe de neutre 1. Si $x \in G$, alors l'ensemble des entiers $n \in \mathbb{Z}$ tels que $x^n = 1$ est un sous-groupe de $\mathbb{Z}$.*

**Proposition 1.4.5** *Soit $G$ un groupe de neutre 1. Si $x \in G$, alors :*
*— soit le sous-groupe engendré par $x$ est infini et dans ce cas les $x^k$ sont deux à deux distincts, $k \in \mathbb{Z}$ ;*
*— soit le sous-groupe engendré par $x$ est d'ordre fini $m$. Dans ce cas, $m$ est le plus petit entier $> 0$ tel que $x^m = 1$, les éléments $1, ..., x^{m-1}$ sont deux à deux distincts et $\langle x \rangle = \{1, ..., x^{m-1}\}$.*

**Définition 7** *Un groupe fini $G$ d'ordre $n$ de la forme $G = \langle x \rangle$ est appelé un groupe cyclique d'ordre $n$. On dit que $x$ engendre $G$. Un élément $x$ dans un groupe tel que $\langle x \rangle$ est fini d'ordre $n$ est appelé un élément d'ordre $n$.*

**Exemples :** La matrice $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ est d'ordre 6 dans $\mathrm{GL}_2(\mathbb{R})$.
En effet, $A^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, $A^3 = -I_2$, $A^4 = -A$, $A = -A^2$, $A^6 = I_2$.
En revanche, la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre infini car $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

*Remarque :* on peut montrer que si $A$ est une matrice à coefficients entiers d'ordre fini $n$, alors $n = 1, 2, 3$ ou 6.

**Exercice 7** *Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique d'ordre $n$, engendré par $\overline{k}$ pour tout entier $k$ premier à $n$.*

**Exercice 8** *Le groupe* $\boldsymbol{\mu}_n$ *est cyclique d'ordre* $n$*, engendré par* $\mathrm{e}^{2ik\pi/n}$ *pour tout entier* $k$ *premier* $n$.

Plus généralement, si $G$ est un groupe, on peut parler du sous-groupe de $G$ engendré par une partie $X$ de $G$. On le note $\langle X\rangle$. C'est le sous-groupe formé par les produits d'une chaîne finie d'éléments de $X$ et d'inverses d'éléments de $X$.

Si $X = \{x_1, ..., x_n\}$ est fini, on note $\langle x_1, ..., x_n\rangle$ le groupe engendré par $X$. On dit aussi que $x_1, ..., x_n$ engendrent $\langle x_1, ..., x_n\rangle$.

Dans ce cas, on a :

$$\langle x_1, ..., x_n\rangle = \{x_{i_1}^{\epsilon_1}...x_{i_k}^{\epsilon_k} \ : \ k \geq 0, 1 \leq i_1, ..., i_k \leq n, \epsilon_1, ..., \epsilon_k = \pm 1\} \ .$$

**Exemples :** le groupe $S_3$ est engendré par $s_1, s_2$, le groupe $Q_8$ est engendré par $I, J$.

**Exercice 9** *Tout sous-groupe de* $\mathbb{Q}$ *de type fini (c-à-d qui peut être engendré par un nombre fini d'éléments) est de la forme* $r\mathbb{Z}$ *pour un certain* $r \in \mathbb{Q}$.

## 1.5 Morphismes de groupes

**Définition 8** *Soient* $G, G'$ *deux groupes. Une application* $\phi : G \to G'$ *est un morphisme de groupes si :*

$$\phi(ab) = \phi(a)\phi(b)$$

*pour tous* $a, b \in G$.

**Exemples :**

— l'application $\mathbb{C}^\times \to \mathbb{C}^\times$, $z \mapsto z^n$ pour un entier $n$,

— l'exponentielle $(\mathbb{R}, +) \to \mathbb{R}^\times$, $x \mapsto \exp x$,

— le logarithme $\mathbb{R}^\times \to \mathbb{R}$, $x \mapsto \ln|x|$,

— le déterminant : $\mathrm{GL}_2(\mathbb{C}) \to \mathbb{C}^\times$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc$,

— l'application $\mathbb{R} \to \mathbb{C}^\times$, $x \mapsto \cos x + i \sin x$,

— l'application $(\mathbb{Z}, +) \to G$, $n \mapsto x^n$, pour un groupe $G$ et un élément fixé $x$ de $G$,

— l'inclusion $H \to G$, $x \mapsto x$ pour un sous-groupe $H$ d'un groupe $G$

sont des morphismes de groupes.

**Proposition 1.5.1** *Si* $\phi : G \to G'$ *est un morphisme de groupes, alors* $\phi(1_G) = 1_{G'}$.

**Définition 9 (noyau et image)** *Soit $\phi : G \to G'$ un morphisme de groupes. On note*

$$\mathrm{Im}\,\phi := \{y \in G' \ : \ ^{\exists}x \in G, y = \phi(x)\}$$

*c'est un sous-groupe de $G'$ (exo) , c'est l'image de $\phi$.*

*On note*

$$\ker\phi := \{x \in G \ : \ \phi(x) = 1\} = \phi^{-1}\{1\}$$

*c'est un sous-groupe de $G$, appelé noyau de $\phi$.*

**Remarque :** plus généralement, si $H'$ est un sous-groupe de $G'$, alors $\phi^{-1}(H')$ est un sous-groupe de $G$.

**Exemples :**

— le noyau de $\mathbb{R} \to \mathbb{C}^\times$, $x \mapsto \cos x + i \sin x$ est $2\pi\mathbb{Z}$ et son image est le sous-groupe des nombres complexes de module 1 ;

— le noyau de dét : $\mathrm{GL}_2(\mathbb{C}) \to \mathbb{C}^\times$ est le groupe spécial linéaire d'indice 2, noté $\mathrm{SL}_2(\mathbb{C})$ ;

— le noyau de $\mathbb{R}^\times \to \mathbb{R}^\times$, $x \mapsto x^2$ est $\{\pm 1\}$ et son image est le sous-groupe des nombres réels strictement positifs ;

— si $n$ est un entier $> 1$, le noyau du morphisme $\mathbb{C}^\times \to \mathbb{C}^\times$, $z \mapsto z^n$ est le sous-groupe des racine $n-$ièmes de l'unité $\boldsymbol{\mu}_n$.

**Remarque :** un morphisme de groupes est injectif $\Leftrightarrow$ son noyau est trivial.

### 1.5.1 Sous-groupes distingués

Le noyau d'un morphisme de groupes $\phi : G \to G'$ possède une propriété remarquable :

$$^{\forall}x \in \ker\phi, ^{\forall}g \in G, \ gxg^{-1} \in \ker\phi \ .$$

**Définition 10** *Si $H$ est un sous-groupe de $G$, on dit que $H$ est distingué dans $G$ si pour tout $g \in G$, tout $h \in H$, $ghg^{-1} \in H$.*

*Le noyau d'un morphisme est toujours distingué.*

**Exemples :** — Dans un groupe abélien, tous les sous-groupes sont distingués ;

— le sous-groupe des rotations est distingué dans $O_2$ ;

— le sous-groupe $\mathrm{SL}_2(\mathbb{C})$ est distingué dans $\mathrm{GL}_2(\mathbb{C})$ ;

— le sous-groupe des matrices diagonales n'est pas distingué dans $\mathrm{GL}_2(\mathbb{C})$.

**Exercice 10** *Soit $D_n$ le sous-groupe de* $\mathrm{GL}_2(\mathbb{C})$ *engendré par les matrices* $\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. *Montrer que $D_n$ est fini d'ordre $2n$ et qu'il contient un sous-groupe cyclique distingué d'ordre $n$. C'est le groupe diédral d'ordre $2n$.*

**Définition 11** *Si $G$ est un groupe, on note :*

$$Z(G) := \{x \in G \ : \ ^{\forall}g \in G, gx = xg\} \ .$$

*C'est un sous-groupe de $G$ appelé le centre de $G$.*

**Remarque :** le centre de $G$ est distingué dans $G$.

**Exemple :** le centre de $\mathrm{GL}_2(\mathbb{C})$ est formé des matrices $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, $\lambda \in \mathbb{C}$.

### 1.5.2 Isomorphismes

Soit $U$ l'ensemble des matrices de la forme $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, $x \in \mathbb{C}$. On vérifie facilement que $U$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$.

De plus, pour tous $x, y \in \mathbb{C}$, on a :

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$$

donc multiplier de telles matrices revient à faire des additions dans $\mathbb{C}$. Plus précisément, l'application bijective :

$$\mathbb{C} \to U, \, x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

est un morphisme de groupes.

Si $\phi$ est un morphisme de groupes bijectif alors l'application réciproque $\phi^{-1}$ est aussi un morphisme de groupes.

**Définition 12** *Un isomorphisme entre deux groupes $G$ et $G'$ est un morphisme bijectif entre $G$ et $G'$. S'il existe un isomorphisme de groupes $\phi : G \to G'$, on dit que $G$ est isomorphe à $G'$ ce qui se note : $G \simeq G'$. Si $G = G'$ et si $\phi : G \to G$ est un isomorphisme, on dit que $\phi$ est un automorphisme.*

**Exercice 11**

$$(\mathbb{R}, +) \simeq (\mathbb{R}_+^*, \times)$$

$$(\mathbb{Z}/n\mathbb{Z}, +) \simeq \boldsymbol{\mu}_n$$

**Proposition 1.5.2** *Tout groupe cyclique d'ordre $n$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

*Démonstration* : Soit $G$ un groupe cyclique d'ordre $n$ engendré par un élément $x$. Alors, l'application :

$$\mathbb{Z}/n\mathbb{Z}\ k + n\mathbb{Z} \mapsto x^k$$

est bien définie et c'est un isomorphisme de groupes. q.e.d.

**Exercice 12** *Montrer que l'ensemble des matrices $2 \times 2$ réelles inversibles de la forme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ isomorphe à $\mathbb{C}^\times$.*

*Montrer l'ensemble des matrices $2\times2$ réelles de la forme $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, $\theta \in \mathbb{R}$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ isomorphe à $S^1$ le groupe des nombres complexes de module 1.*



**Exemples :** l'application $\overline{0} \mapsto \overline{0}$, $\overline{1} \mapsto \overline{2}$, $\overline{2} \mapsto \overline{1}$ est un automorphisme de $\mathbb{Z}/3\mathbb{Z}$ ;

— l'application $A \mapsto {}^tA^{-1}$ est un automorphisme de $\mathrm{GL}_2(\mathbb{C})$ ;

— si $G$ est un groupe et si $g \in G$ est un élément fixé, l'application $x \mapsto gxg^{-1}$ est un automorphisme de $G$. Un tel automorphisme est appelé un *automorphisme intérieur.*

## 1.6 Classes à gauche et à droite

Soient $G$ un groupe et $H$ un sous-groupe de $G$.

**Définition 13** *Une classe à gauche est une partie de $G$ de la forme :*

$$gH := \{gh\ :\ h \in H\}$$

*pour un certain $g \in G$.*

Par exemple le sous-groupe $H$ lui-même est une classe à gauche : celle de 1 (et plus généralement celle de $h$ pour tout $h \in H$).

**Proposition 1.6.1** *Si $x, y \in G$, alors $xH = yH \Leftrightarrow y^{-1}x \in H \Leftrightarrow x \in yH \Leftrightarrow y \in xH \Leftrightarrow xH \cap yH \neq \emptyset$.*

**Corollaire 1.6.1.1** *Les classes à gauche forment une partition de $G$.*

**Notation :** on note $G/H$ l'ensemble des classes à gauche $gH$, $g \in G$.

Le nombre de classes à gauche, s'il est fini, est appelé *l'indice* de $H$ dans $G$ et noté $[G : H]$.

**Remarque :** on peut définir aussi des classes à droite. L'application $gH \mapsto Hg$ est une bijection entre l'ensemble des classes à gauche et l'ensemble des classes à droite.

**Proposition 1.6.2** *Le sous-groupe $H$ est distingué si et seulement si $gH = Hg$ pour tous $g \in G$.*

**Remarque :** si $g \in G$ est fixé, alors l'application $H \to gH$, $h \mapsto gh$ est bijective ; donc si $H$ est fini, toutes les classes à gauche ont $|H|$ éléments.

**Corollaire 1.6.2.1 (théorème de Lagrange)** *Si $G$ est un groupe fini et si $H$ est un sous-groupe de $G$, alors $|H|$ divise $|G|$.*

*Démonstration* : $|G| = |H|[G : H]$. *q.e.d.*

**Conséquence :** l'ordre d'un élément divise l'ordre du groupe (dans un groupe fini $G$). En particulier, si $G$ est un groupe fini, $x^{|G|} = 1$ pour tout $x \in G$.

**Exemple :** dans $S_3$ tous les éléments ont un ordre qui divise 6 (en fait, $1, 2$ et 3 sont les seules possibilités).

**Exercice 13** *Soit $p$ un nombre premier. Si $G$ est un groupe d'ordre $p$, alors $G$ est cyclique et tout $1 \neq g \in G$ engendre $G$.*

**Proposition 1.6.3** *Si $G$ est cyclique d'ordre $n$, alors pour tout $d|n$ il existe un unique sous-groupe de $G$ d'ordre $d$ et ce sous-groupe est cyclique. De plus tout sous-groupe de $G$ est cyclique.*

**Exercice 14** *Les seuls sous-groupes finis de $\mathbb{C}^\times$ sont les groupes de racines de l'unité $\boldsymbol{\mu}_n$, $n > 0$.*

## 1.7 Le groupe symétrique

L'ensemble des permutations de l'ensemble $\{1, ..., n\}$ muni de la loi de compositon des applications est un groupe appelé *groupe symétrique* d'indice $n$ et noté $S_n$.

**Proposition 1.7.1** *Si $G$ est un groupe fini, alors $G$ est isomorphe à un sous-groupe de $S_n$ pour un $n$ assez grand.*

*Démonstration :* Soit $G = \{g_1, ..., g_n\}$ un groupe fini d'ordre $n$. Soit $g \in G$. Pour tout $i$, il existe un unique entier $1 \leq k \leq n$ tel que $g_k = gg_i$ ; on pose $\sigma_g(i) := k$. Alors $\sigma_g \in S_n$ et $G \to S_n$, $g \mapsto \sigma_g$ est un morphisme injectif de groupes. q.e.d.

**Exemple :** dans $S_4$, la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$ est aussi notée $(2, 3)$.

Plus généralement si $1 \leq i_1, ..., i_k \leq n$, sont des entiers deux à deux distincts, on note :

$$(i_1, ..., i_k)$$

la permutation qui envoie $i_1$ sur $i_2$, $i_2$ sur $i_3$, ..., $i_k$ sur $i_1$ et laisse fixe tous les entiers $j \notin \{i_1, .., i_k\}$.

On dit qu'une telle permutation est un *cycle de longueur $k$* ou un *$k-$cycle*.

Un cycle de longueur 1 est l'identité. Un cycle de longueur 2 est aussi appelé une *transposition* .

**Exemple :** dans $S_3$, il y a 3 transpositions : $(1, 2)$, $(2, 3)$, $(1, 3)$ et 2 $3-$cycles : $(1, 2, 3)$ et $(1, 3, 2)$.

**Remarque :** on a bien sûr : $(1, 2, 3) = (2, 3, 1) = (3, 1, 2)$.

**Exercice 15** *Vérifier que dans $S_n$, le cycle $(i_1, ..., i_k)$ est un élément d'ordre $k$.*

**Remarque :** pour tout $\sigma \in S_n$, on a :

$$\sigma(i_1, ..., i_k)\sigma^{-1} = (\sigma(i_1), ..., \sigma(i_k)) \ .$$

### 1.7.1 Décomposition en cycles

Soit $\sigma \in S_n$ une permutation. Le *support* de $\sigma$ est l'ensemble des $1 \leq x \leq n$ tel que $\sigma(x) \neq x$.

**Exercice 16** *Vérifier que si $\sigma, \tau \in S_n$ sont des permutations à supports disjoints, alors $\sigma\tau = \tau\sigma$.*

**Proposition 1.7.2** *Toute permutation se décompose en un produit de cycles à supports disjoints. Cette décomposition est unique à permutation près de l'ordre des cycles.*

**Exemple :** soit $\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$. Alors $\sigma = (1,5)(2,4)$.

*Démonstration :* Soit $\sigma \in S_n$. Si $1 \leq k \leq n$, on pose :

$$\mathscr{O}_k := \{\sigma^l(k) \ : \ l \in \mathbb{Z}\} \ .$$

Comme $\{1, ..., n\}$ est fini, $\mathscr{O}_k = \{k, ..., \sigma^{l-1}(k)\}$ où $l$ est le plus petit entier $> 0$ tel que $\sigma^l(k) = k$. On a aussi $l = |\mathscr{O}_k|$.

Si $1 \leq k, k' \leq n$, alors $\mathscr{O}_k = \mathscr{O}_{k'}$ ou $\mathscr{O}_k \cap \mathscr{O}_{k'} = \emptyset$. Les ensembles $\mathscr{O}_k$ forment donc une partition de $\{1, ..., n\}$. Soient $k_1, ..., k_r$ des entiers tels que les ensembles $\mathscr{O}_{k_i}$ soient deux à deux distincts et tels que :

$$\{1, ..., n\} = \mathscr{O}_{k_1} \cup ... \cup \mathscr{O}_{k_r} \ .$$

Posons $n_i := |\{\mathscr{O}_{k_i}\}|$ pour tout $i$. Alors :

$$\mathscr{O}_{k_i} = \{k_i, \sigma(k_i), ..., \sigma^{n_i - 1}(k_i)\}$$

et :

$$\sigma = (k_1, \sigma(k_1), ..., \sigma^{n_1-1}(k_1))...(k_r, \sigma(k_r), ..., \sigma^{n_r-1}(k_r))$$

*q.e.d.*

**Corollaire 1.7.2.1** *L'ensemble des transpositions engendre $S_n$.*

*Démonstration :* Il suffit de remarquer qu'un cycle est un produit de transpositions :

$$(i_1, ..., i_k) = (i_1, i_2)(i_2, i_3)....(i_{k-1} i_k) \ .$$

*q.e.d.*

**Remarque :** par exemple : $(1,2,3) = (1,2)(2,3) = (2,3)(1,2)(2,3)(1,2)$. La décomposition en produit de transpositions n'est pas unique, ni le nombre de transpositions mais la parité du nombre de transpositions est unique (*cf.* plus loin ...). Autre exemple : $(1,3) = (1,2)(2,3)(1,2)$.

**Corollaire 1.7.2.2** *Les transpositions $(i, i+1)$, $1 \leq i \leq n-1$, engendrent $S_n$.*

*Démonstration :* Il suffit de vérifier qu'une transposition quelconque est un produit de transpositions de la forme $(i, i+1)$. Or, si $1 \leq i < j \leq n$, on a :

$$(i, j) = s_i s_{i+1} ... s_{j-2} s_{j-1} s_{j-2} ... s_{i+1} s_i$$

où pour tout $1 \leq k \leq n-1$, $s_k$ est la transposition $(k, k+1)$. <u>*q.e.d.*</u>

**Exercice 17** *Les transpositions* $(1, i)$, $2 \leq i \leq n$ *engendrent* $S_n$.

### 1.7.2 Signature

Soit $\sigma \in S_n$. Une *inversion* de $\sigma$ est une paire $\{i, j\}$ telle que $i < j$ et $\sigma(i) > \sigma(j)$.

*« Le nombre d'inversions de* $\sigma$ *est le nombre de fois où, dans la liste* $\sigma(1), ..., \sigma(n)$*, un entier plus grand apparaît à gauche d'un plus petit. »*

EXEMPLE : Voici les inversions et les signatures des 6 permutations $\sigma \in \mathscr{S}_3$ :

| $\sigma$ | $I(\sigma)$<br>$\#I(\sigma)$ | $\epsilon(\sigma)$ |
|---|---|---|
| Id : $1 \mapsto 1$, $2 \mapsto 2$, $3 \mapsto 3$ | $\emptyset$<br>0 | 1 |
| $s_1$ : $1 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 3$ | {{1,2}}<br>1 | $-1$ |
| $s_2$ : $1 \mapsto 1$, $2 \mapsto 3$, $3 \mapsto 2$ | {{2,3}}<br>1 | $-1$ |
| $s_1 s_2$ : $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$ | {{2,3},{1,3}}<br>2 | 1 |
| $s_2 s_1$ : $1 \mapsto 3$, $2 \mapsto 1$, $3 \mapsto 2$ | {{1,2},{1,3}}<br>2 | 1 |
| $s_1 s_2 s_1$ $(= s_2 s_1 s_2)$ : $1 \mapsto 3$, $2 \mapsto 2$, $3 \mapsto 1$ | {{1,2},{2,3},{1,3}}<br>3 | $-1$ |

*Le nombre d'inversions d'une permutation est aussi le nombre de « croisements » dans le diagramme qui la représente.*

**Exemple :** les inversions de la transposition $(r, s)$, $r < s$, sont les paires :

$$\{r, r+1\}, ..., \{r, s-1\}, \{r, s\}, \{r+1, s\}, ..., \{s-1, s\}$$

ce qui fait $2(s-r)-1$ inversions.

**Définition 14** *Si $\sigma$ est une permutation avec un nombre pair (respectivement impair) d'inversions, on dit que c'est une permutation paire (respectivement impaire). On définit $\epsilon(\sigma) := (-1)^{\text{nombre d'inversions de } \sigma}$ ; c'est la signature de $\sigma$.*

**Exemple :** les transpositions sont de signature $-1$.

**Lemme 1.7.3** *Soit $\sigma \in S_n$ et soit $\tau$ une transposition. Alors $\epsilon(\sigma\tau) = \epsilon(\tau\sigma) = -\epsilon(\sigma)$.*

*Démonstration du lemme :*

Soient $I(\sigma)$ l'ensemble des inversions de $\sigma$. On a une bijection :

$$(I(\sigma\tau) \setminus I(\sigma)) \cup (I(\sigma) \setminus I(\sigma\tau)) \overset{1:1}{\longleftrightarrow} I(\sigma\tau\sigma^{-1})$$

$$\{i, j\} \mapsto \{\sigma(i), \sigma(j)\}$$



(*exo*) .

Or, $\sigma\tau\sigma^{-1}$ est une transposition : c'est la transposition qui échange $\sigma(i)$ et $\sigma(j)$. Donc $|I(\sigma\tau\sigma^{-1})|$ est impair. Or :

$$|I(\sigma)| = |I(\sigma) \cap I(\sigma\tau)| + |I(\sigma) \setminus I(\sigma\tau)|$$

$$|I(\sigma\tau)| = |I(\sigma) \cap I(\sigma\tau)| + |I(\sigma\tau) \setminus I(\sigma)|$$

$$\Rightarrow |I(\sigma)| + |I(\sigma\tau)| = 2|I(\sigma) \cap I(\sigma\tau)| + |I(\sigma) \setminus I(\sigma\tau)| + |I(\sigma\tau) \setminus I(\sigma)|$$

$$\Rightarrow |I(\sigma)| + |I(\sigma\tau)| = 2|I(\sigma) \cap I(\sigma\tau)| + |I(\sigma\tau\sigma^{-1})|$$

et $|I(\sigma)| + |I(\sigma\tau)|$ est impair. Donc $\epsilon(\sigma) = -\epsilon(\sigma\tau)$. *q.e.d.*

**Exercice 18** *On note $s_i$ la transposition $(i, i+1)$. Redémontrer le lemme en montrant que si $\sigma(i) < \sigma(i+1)$, alors :*

$$I(\sigma s_i) = \{\{s_i(k), s_i(l)\} \ : \ \{k, l\} \in I(\sigma)\} \cup \{i, i+1\} \ .$$

En particulier si $\sigma$ est un produit de $p$ transpositions, $\epsilon(\sigma) = (-1)^p$. On en déduit donc qu'un $k-$cycle a pour signature $(-1)^{k-1}$.

**Proposition 1.7.4** *La signature $\epsilon : S_n \to \{\pm 1\}$ est un morphisme de groupes.*

**Définition 15** *L'ensemble des permutations paires est le noyau de la signature. C'est donc un sous-groupe distingué de $S_n$. On le note $A_n$ : c'est le groupe alterné d'indice $n$. .*

**Notation :** $A_n := \ker \epsilon$.
**Exemple :** le groupe $A_3$ a trois éléments : $1, (1, 2, 3), (1, 3, 2)$.

**Exercice 19** *Si $n \geq 3$, le groupe $A_n$ est engendré par les $3-$cycles $(1, 2, i)$, $3 \leq i \leq n$.*

Comme $\epsilon$ est un morphisme, on en déduit que $\epsilon(\sigma) = \epsilon(\sigma^{-1})$ pour toute permutation $\sigma$.
En fait on a même plus :

**Exercice 20** *Vérifier qu'il y a une bijection entre $I(\sigma)$ et $I(\sigma^{-1})$.*

**Proposition 1.7.5** *La signature est le seul morphisme non trivial de $S_n$ vers $\mathbb{C}^\times$.*

*Démonstration :* Une transposition est d'ordre 2 et donc son image par un morphisme dans $\mathbb{C}^\times$ est $\pm 1$. De plus, toutes les transpositions sont conjuguées [†] et engendrent $S_n$. *q.e.d.*

†. On dit que deux éléments $x$ et $y$ d'un groupe $G$ sont *conjugués* s'il existe $g \in G$ tel que $y = gxg^{-1}$.

# Chapitre 2

# Rappels sur les matrices

**Définition 16** *Une matrice $m \times n$ à coefficients dans $\mathbb{K}$ est un « tableau » de nombres $\in \mathbb{K}$ à $m$ lignes et $n$ colonnes. Notation : $\mathscr{M}_{m,n}(\mathbb{K})$.*

**Notation :** On note $a_{i,j}$ le coefficient de la ligne $i$ et de la colonne $j$.

EXEMPLE : *Triangles de Pascal.* Voici 3 exemples de matrices de taille $n+1 \times n+1$ :

$$T_- := \begin{pmatrix} 1 & 0 & \dots & & & & 0 \\ 1 & 1 & \ddots & & & & \vdots \\ 1 & 2 & 1 & & & & \\ 1 & 3 & 3 & 1 & & & \\ 1 & 4 & 6 & 4 & 1 & & \\ \vdots & & & & & \ddots & 0 \\ 1 & n & \dots & & & & 1 \end{pmatrix} = \left( \binom{i}{j} \right)_{0 \leq i,j \leq n}$$

$$T_+ := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 2 & 3 & 4 & & n \\ \vdots & & 1 & 3 & 6 & & \vdots \\ & & & 1 & 4 & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ 0 & \dots & & & & & 1 \end{pmatrix} = \left( \binom{j}{i} \right)_{0 \leq i,j \leq n}$$

$$P := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 3 & 4 & & & n+1 \\ 1 & 3 & 6 & & & & \\ 1 & 4 & & \ddots & & & \\ 1 & & & & & & \\ \vdots & & & & & & \\ 1 & n+1 & & & & & \binom{2n}{n} \end{pmatrix} = \left(\binom{i+j}{i}\right)_{0 \leq i,j \leq n}$$

### 2.0.3 Opérations

— On peut additionner deux matrices de même taille (addition terme à terme) ;

— On peut multiplier une matrice par un scalaire $\lambda$ (tous les coefficients sont multipliés par $\lambda$) ;

— On peut multiplier une matrice $A$ de taille $m \times n$ par une matrice $B$ de taille $n \times p$ pour obtenir une matrice $C = AB$ de taille $m \times p$ :

$$c_{i,j} := \sum_{k=1}^{n} a_{i,k} b_{k,j}$$

« le coefficient $(i, j)$ de la matrice $AB$ est le produit scalaire de la ligne $i$ de $A$ par la colonne $j$ de $B$. ».

**Exercice 21** — *matrices de rotations :*

$$\begin{pmatrix} \cos a & -\sin a \\ \sin a & \cos a \end{pmatrix} \cdot \begin{pmatrix} \cos b & -\sin b \\ \sin b & \cos b \end{pmatrix}$$

$$= \begin{pmatrix} \cos(a+b) & -\sin(a+b) \\ \sin(a+b) & \cos(a+b) \end{pmatrix}$$

— *nombres complexes*

$$\begin{pmatrix} \mathrm{Re} z & -\mathrm{Im}\, z \\ \mathrm{Im}\, z & \mathrm{Re} z \end{pmatrix} \cdot \begin{pmatrix} \mathrm{Re} z' & -\mathrm{Im}\, z' \\ \mathrm{Im}\, z' & \mathrm{Re} z' \end{pmatrix}$$

$$= \begin{pmatrix} \mathrm{Re}(zz') & -\mathrm{Im}\,(zz') \\ \mathrm{Im}\,(zz') & \mathrm{Re}(zz') \end{pmatrix}$$

— *matrices de Pascal*

$$T_{-}T^{+} = P$$

*indication : $P_{i,j}$ est le coefficient de degré $j$ du polynôme $(1+X)^{i+j}$. Or, $(1+X)^{i+j} = (1+X)^i(1+X)^j$ ; exprimer le polynôme $(1+X)^i$ (respectivement $(1+X)^j$) en fonction des coefficients de $T_{-}$ (respectivement $T^{+}$).*

**Proposition 2.0.6 (Associativité)** *Soient $A$ une matrice de taille $m \times n$, $B$ une matrice de taille $n \times p$ et $C$ une matrice de taille $p \times q$. Alors on a l'égalité de matrices $m \times q$ :*

$$(AB)C = A(BC)$$

*Démonstration :* Notons $u_{i,j}$ les coefficients du membre de gauche et $v_{i,j}$ ceux du membre de droite. Alors :

$$u_{i,j} = \sum_{\substack{1\le k\le n \\ 1\le l\le p}} a_{i,k}b_{k,l}c_{l,j} = v_{i,j} \ .$$

q.e.d.

## 2.1 Matrices carrées

$$\begin{pmatrix} \ddots & \ldots & (i<j) \\ \vdots & (i=j) & \vdots \\ (i>j) & \ldots & \ddots \end{pmatrix}$$

— Propriétés de $\mathbb{K}-$algèbre :
*distributivité*

$$A(B+C) = AB + AC \ , \ (A+B)C = AB + BC \ ,$$

$$\forall t \in \mathbb{K},\ t(A)B = A(tB) = t(AB)$$

— Propriétés « négatives » :
*non commutativité :*

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = 0 \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

*existence d'éléments nilpotents non nuls :*

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = 0$$

— Effet de la multiplication à gauche ou à droite par une matrice diagonale :

$$\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}\begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & & a_{n,n} \end{pmatrix} = \begin{pmatrix} d_1a_{1,1} & \dots & d_1a_{1,n} \\ \vdots & & \vdots \\ d_na_{n,1} & & d_na_{n,n} \end{pmatrix} \tag{2.1}$$

$$\begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & & a_{n,n} \end{pmatrix}\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix} = \begin{pmatrix} d_1a_{1,1} & \dots & d_na_{1,n} \\ \vdots & & \vdots \\ d_1a_{n,1} & & d_na_{n,n} \end{pmatrix} \tag{2.2}$$



**Définition 17** *La matrice identité, notée $I_n$ :*

$$I_n := \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$$

*« Des 1 sur la diagonale, des 0 en dehors ».*

D'après 2.1 et 2.2,

$$\forall A \in \mathscr{M}_n(\mathbb{K}),\ AI_n = I_nA = A\ .$$

**Définition 18** *Matrices inversibles. Une matrice $A \in \mathscr{M}_n(\mathbb{K})$ est inversible s'il existe une matrice, notée $A^{-1}$, telle que :*

$$AA^{-1} = A^{-1}A = I_n\ .$$

*Notation :* $\mathrm{GL}_n(\mathbb{K})$ *est l'ensemble des matrices $n \times n$ inversibles à coefficients dans $\mathbb{K}$.*

**Remarque :** $\mathrm{GL}_n(\mathbb{K})$ est un groupe pour la multiplication : c'est le *groupe général linéaire.*

**Remarque :** $AB = I_n \Rightarrow BA = I_n$ (non trivial !)

#### 2.1.0.1 La transposée

**Définition 19** $^t(A)_{i,j} := A_{j,i}$ *« Les lignes de* $^tA$ *sont les colonnes de* $A$ *(et vice versa) ».*

**Propriétés :**

$$^t(tA) = t\,^tA,\ \ ^t(A+B) = {}^tA + {}^tB\ ,\ ^t(AB) = {}^tB\,^tA$$

## 2.2 Applications

### 2.2.1 La suite de Fibonacci

C'est la suite :

$$0, 1, 1, 2, 3, 5, 8, 13, ...$$

$$f_0 := 0, f_1 := 1, \forall n \geq 1,\ f_{n+1} = f_n + f_{n-1}$$

**Problème :** exprimer $f_n$ en fonction de $n$.

**Solution :** On remarque que :

$$\forall n \geq 1, \begin{pmatrix} f_n \\ f_{n+1} \end{pmatrix} = A \begin{pmatrix} f_{n-1} \\ f_n \end{pmatrix}$$

où $A$ est la matrice

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

et donc :

$$\forall n \geq 0, \begin{pmatrix} f_n \\ f_{n+1} \end{pmatrix} = A^n \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad .$$

Vérifier que :

$$\forall n \geq 1,\ A^n = \begin{pmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{pmatrix} \quad .$$

Pour calculer $A^n$, on introduit :

$$\delta := \frac{1+\sqrt{5}}{2},\ \overline{\delta} := \frac{1-\sqrt{5}}{2},\ P := \begin{pmatrix} 1 & 1 \\ \delta & \overline{\delta} \end{pmatrix},\ P^{-1} = \frac{1}{\sqrt{5}} \begin{pmatrix} -\overline{\delta} & 1 \\ \delta & -1 \end{pmatrix}$$

(« pourquoi ? patience ! »)
et on remarque que :

$$A = PDP^{-1}$$

où $D := \begin{pmatrix} \delta & 0 \\ 0 & \overline{\delta} \end{pmatrix}$.

On trouve donc :

$$\forall n \geq 0,\ A^n = PD^nP^{-1}$$

$$\forall n \geq 0,\ A^n = P \begin{pmatrix} \delta^n & 0 \\ 0 & \overline{\delta}^n \end{pmatrix} P^{-1}$$

et donc :

$$\forall n \geq 0,\ f_n = A^n_{1,2} = \frac{\delta^n - \overline{\delta}^n}{\sqrt{5}}\ .$$

**Remarque :** Les nombres $(\frac{1+\sqrt{5}}{2})$ et $(\frac{1-\sqrt{5}}{2})$ sont les *valeurs propres* de $A$ (définition à venir ...).

### 2.2.2 Graphes

Un pilote voyage entre trois villes suivant le graphe suivant :

$$P \rightleftarrows B \longrightarrow M$$

1 2 3

Les flèches représentent les trajets possibles à chaque étape.

**Question :** En $n$ étapes, combien y a-t-il de façons d'aller de $i$ à $j$ ?

**Réponse :** Notons $b_{i,j,n}$ le nombre cherché. On pose $A$ la matrice d'incidence du graphe *i.e.*

$$a_{i,j} := \begin{cases} 1 \text{ s'il y a une flèche de } i \text{ vers } j \\ 0 \text{ sinon.} \end{cases}$$

Ici :

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

On a $b_{i,j,n} = A^n_{i,j}$. *Démonstration :* Par récurrence sur $n \geq 1$ :

$$b_{i,j,n} = \sum_k b_{i,k,n-1} b_{k,j,1} = \sum_k A^{n-1}_{i,k} A_{k,j}$$

$$= A^n_{i,j} \ .$$

En particulier, si on sait calculer $A^n$ (*cf.* suite du cours), on peut vérifier qu'un pilote qui part de $P$ atterrira, au bout d'une infinité d'étapes, $\rho^2$ fois plus souvent à $M$ qu'à $B$ avec :

$$\rho^2 := \lim_{n\infty} \frac{A^n_{1,3}}{A^n_{1,2}} \approx 1,75...$$

où $\rho$ est l'unique racine réelle de $X^3 - X - 1$.

Ici encore, $\rho$ est une *valeur propre* de $A$.

### 2.2.3 Équation différentielle

**Problème :** Résoudre l'équation différentielle :

$$(E) \ y'' + k^2 y = 0$$

où $0 \neq k \in \mathbb{R}$.

**Solution :** On pose $Y := \begin{pmatrix} y \\ y' \end{pmatrix}$. On a :

$$(E) \Leftrightarrow Y' = AY$$

où $A$ est la matrice :

$$\begin{pmatrix} 0 & 1 \\ -k^2 & 0 \end{pmatrix}$$

or, nous verrons plus loin que :

$$Y' = AY \Leftrightarrow Y(t) = e^{tA} Y(0)$$

où $e^{tA}$ est une matrice définie de la même manière que l'exponentielle complexe.

Ici :

$$e^{tA} = \begin{pmatrix} \cos(kt) & \frac{\sin(kt)}{k} \\ -k\sin(kt) & \cos(kt) \end{pmatrix} .$$

Donc :

$$\forall t,\ y(t) = y(0)\cos(kt) + \frac{y'(0)}{k}\sin(kt) .$$

<u>*q.e.d.*</u>

## 2.3 Systèmes linéaires

Les matrices permettent d'écrire de façon condensée les systèmes d'équations linéaires :

$$\left\{ \begin{array}{rcl} a_{1,1}x_1 + \dots + a_{1,n}x_n & = & b_1 \\ \dots & & \\ a_{m,1}x_1 + \dots + a_{m,n}x_n & = & b_n \end{array} \right. \Leftrightarrow AX = B$$

où

$$A = (a_{i,j})_{\substack{1\le i\le m \\ 1\le j\le n}},\ B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix},\ X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} .$$

## 2.4 Rang d'une matrice

### 2.4.1 Rappels sur les espaces vectoriels

Soit $E$ un $\mathbb{K}-$espace vectoriel *c-à-d* :

$E$ est un ensemble muni d'une addition $+$ et d'une multiplication par les éléments de $\mathbb{K}$ (appelés scalaires) telles que :

1. $(E, +)$ est un groupe abélien *i.e.* :
   - $\forall x, y, z \in E,\ x + (y + z) = (x + y) + z$ ;
   - $\forall x, y \in E,\ x + y = y + x$ ;
   - $\exists 0 \in E,\ \forall x \in E,\ x + 0 = 0 + x = x$ ;

– $^\forall x \in E$, $^\exists(-x) \in E$, $x + (-x) = (-x) + x = 0$ ;

2. $^\forall \lambda \in \mathbb{K}$, $^\forall x, y \in E$, $\lambda(x + y) = \lambda x + \lambda y$ ;
3. $^\forall \lambda, \mu \in \mathbb{K}$, $^\forall x \in E$, $(\lambda + \mu)x = \lambda x + \mu x$ ;
4. $^\forall \lambda, \mu \in \mathbb{K}$, $^\forall x \in E$, $(\lambda\mu)x = \lambda(\mu x)$ ;
5. $^\forall x \in E$, $1x = x$.

Les éléments de $E$ sont appelés des *vecteurs*.

Exemple : [de base] $E = \mathbb{K}^n$ muni de l'addition :

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

et de la multiplication par les scalaires :

$$\lambda \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}$$

pour tous $\lambda, x_1, ..., y_1, ... \in \mathbb{K}$.

Soient $v_1, ..., v_m$ des vecteurs de $E$.

Une *combinaison linéaire* des vecteurs $v_1, ..., v_m$ est un vecteur de la forme :



$$t_1 v_1 + ... + t_m v_m$$

où $t_1, ..., t_m \in \mathbb{K}$.

On dit que $v_1, ..., v_m$ sont $\mathbb{K}-$*linéairement indépendants* (ou *libres*) si :

$$^\forall t_1, ..., t_m \in \mathbb{K},\ t_1 v_1 + ... + t_m v_m = 0 \Rightarrow t_1 = ... = t_m = 0$$

sinon, on dit qu'ils sont *liés*.

On dit que $v_1, ..., v_m$ sont générateurs (de $E$) ou qu'ils engendrent $E$ si tout vecteur de $E$ est une combinaison linéaire de $v_1, ..., v_m$.

Si les vecteurs $v_1, ..., v_m$ sont à la fois libres et générateurs on dit qu'ils forment une *base* de $E$.

Exemple : *La base canonique de* $\mathbb{K}^n$ *est la base formée des vecteurs :*

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, ..., \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

**Proposition 2.4.1** *Soit* $v_1, ..., v_n$ *une base de* $E$.
*i) Si* $w_1, ..., w_m$ *engendrent* $E$*, alors* $m \geq n$ *;*
*ii) Si* $w_1, ..., w_m$ *sont libres, alors* $m \leq n$ *;*

**Conséquence :**

**Définition 20** *Deux bases de* $E$ *ont le même cardinal. Ce cardinal commun est la dimension de* $E$*, notée* $\dim E$.

**Remarque :** $\dim \mathbb{K}^n = n$. D'après la proposition $n+1$ vecteurs de $\mathbb{K}^n$ sont toujours liés.

*Démonstration :* i : supposons, quitte à diminuer $m$, que pour tout $k$,

$$w_{k+1} \notin \langle w_1, ..., w_k \rangle \ .$$

Il existe $t_1, ..., t_n \in \mathbb{K}$ tels que

$$w_1 = t_1 v_1 + ... + t_n v_n \ .$$

Soit $1 \leq i_1 \leq n$ tel que $t_{i_1} \neq 0$. Alors :

$$v_1, ..., \cancel{v_{i_1}}, ..., v_n, w_1$$

(« dans la liste $v_1, ..., v_n$, on remplace $v_{i_1}$ par $w_1$ ») est encore une base de $E$ (*exo*) . On peut montrer plus généralement, par récurrence sur $k$ que pour tout $1 \leq k \leq \min\{m, n\}$, il existe $1 \leq i_1, ..., i_k \leq n$ deux à deux distincts tels que :

$$v_1, ..., \cancel{v_{i_1}}, ..., , \cancel{v_{i_k}}, ..., v_n, w_1, ..., w_k$$

est encore une base de $E$ (où on a remplacé dans la liste $v_1, ..., v_n$ les vecteurs $v_{i_1}, ..., v_{i_k}$ par les vecteurs $w_1, ..., w_k$).

En particulier, si, par l'absurde, $m < n$, on obtient une base de $E$ de la forme :

$$v_i, w_1, ..., w_m, \ i \in \{1, ..., n\} \setminus \{i_1, ..., i_m\}$$

ce qui est absurde car $\langle w_1, ..., w_m \rangle$ engendre $E$.

Donc $m \geq n$.

ii : On raisonne de la même façon. Il existe $t_1, ..., t_n$ tels que $w_1 = t_1 v_1 + ... + t_n v_n$. Il existe $i_1$ tel que $t_{i_1} \neq 0$. Alors, $w_1, v_1, ..., \cancel{v_{i_1}}, ...v_n$ forment une base de $E$. De même, par récurrence sur $1 \leq k \leq \min_{\{m,n\}}$, on peut montrer qu'il existe $1 \leq i_1, ..., i_k \leq n$ deux à deux distincts tels que les vecteurs :

$$w_1, ..., w_k, v_1, ..., \cancel{v_{i_1}}, ..., \cancel{v_{i_k}}, ...v_n$$

forment une base de $E$. Si (*par l'absurde*), $m > n$, on peut prendre $k = n$ :

$$w_1, ..., w_n$$

forment une base de $E$. Mais cela est absurde car alors $w_m$ $(m > n)$ est une combinaison linéaire de $w_1, ..., w_n$ ce qui contredit l'indépendance linéaire des $w_j$. *q.e.d.*

**Définition 21** *Une application $f : E \to F$ entre deux $\mathbb{K}-$espaces vectoriels est linéaire si :*

$$i)\ {}^{\forall}u, {}^{\forall}v \in E,\ f(u+v) = f(u) + f(v)$$

$$ii)\ {}^{\forall}u \in E, {}^{\forall}t \in \mathbb{K}, f(tu) = tf(u)$$

**Définition 22** *Soit $E$ un $\mathbb{K}-$espace vectoriel. Une partie $F \subseteq E$ est un sous-espace de $E$ si :*

$$0 \in F,\ {}^{\forall}u, v \in F, {}^{\forall}t \in \mathbb{K}, tu \in F \text{ et } u + v \in F$$

Exemple : Soit $f : E \to F$ une application linéaire. Son noyau $\ker f := f^{-1}(\{0\})$ est un sous-espace de $E$ et son image $\operatorname{Im} f := \{y \in F : {}^{\exists}x \in E, y = f(x)\}$ est un sous-espace de $F$.

**Proposition 2.4.2** *Une application linéaire $f : E \to F$ est injective $\Leftrightarrow$* $\ker f = \{0\}$

*Démonstration :* Si $\ker f = 0$, si $f(u) = f(v)$, alors $f(u - v) = 0$ *i.e.* $u - v \in \ker f = 0$ donc $u - v = 0$ *i.e.* $u = v$. *q.e.d.*

**Définition 23** *Le rang d'une famille de vecteurs $v_1, ..., v_n$ dans un espace vectoriel $E$ est la dimension de $\langle v_1, ..., v_n \rangle$, l'espace vectoriel engendré par ces vecteurs.*

Soit $A$ une matrice de taille $m \times n$ à coefficients dans $\mathbb{K}$.
On notera $\underline{A}$, ou simplement $A$, l'application linéaire associée :

$$\underline{A} : \mathbb{K}^n \to \mathbb{K}^m$$

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto AX = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$$

où

$$^\forall 1 \leq i \leq m,\ y_i = \sum_{j=1}^{n} a_{i,j} x_j \ .$$

**Remarque :** Soient $A, B \in \mathscr{M}_{m,n}(\mathbb{K})$. Alors :

$$A = B \Leftrightarrow {}^\forall X \in \mathbb{K}^n,\ AX = BX \ .$$

**Exercice 22** *Soient* $A \in \mathscr{M}_{m,n}(\mathbb{K})$, $B \in \mathscr{M}_{n,p}(\mathbb{K})$. *Soient* $\underline{A} : \mathbb{K}^n \to \mathbb{K}^m$, $\underline{B} : \mathbb{K}^p \to \mathbb{K}^n$ *les applications linéaires associées. Alors* $\underline{AB} = \underline{A} \circ \underline{B}$.

**Définition 24 (image et noyau)** *Soit* $A$ *une matrice* $m \times n$. *Son noyau est le sous-espace (exo) :*

$$\ker A = \left\{ X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n \ : \ AX = 0 \right\}$$

$$\operatorname{Im} A = \left\{ Y = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} \in \mathbb{K}^m \ : \ {}^\exists X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n, Y = AX \right\}$$

**Remarque :** La $j-$ième colonne de $A$ est le vecteur $Ae_j$ où : $e_j$ est le vecteur colonne

$$\begin{pmatrix} \vdots \\ 1 \\ \vdots \end{pmatrix}$$

avec un « 1 » en $j-$ième position et des « 0 » ailleurs.

En particulier, $\operatorname{Im} A$ est le sous-espace de $\mathbb{K}^m$ engendrée par les vecteurs colonnes de $A$.

### 2.4.2 Matrices échelonnées

**Définition 25** *Une matrice échelonnée est une matrice de la forme :*

$$\begin{pmatrix} 0 & \dots & a_{1,j_1} & \dots & & & \\ 0 & \dots & & a_{2,j_2} & \dots & & \\ \vdots & & & & & & \\ & & & & & a_{r,j_r} & \dots \\ 0 & \dots & & & & & 0 \end{pmatrix}$$

*où $0 \leq r \leq n$, pour tout $1 \leq k \leq r$, $a_{k,j_k}$ est le premier terme non nul de la ligne $k$ et $j_1 < \dots < j_r$.*

On appellera opération élémentaire sur les lignes une des opérations suivantes :

— ajouter à une ligne $(i)$ une autre ligne $(j)$ multipliée par un coefficient $t \in \mathbb{K}$ ;

— échanger deux lignes : $i$ et $j$ ;

— multiplier la ligne $i$ par un coefficient non nul $\alpha \in \mathbb{K}^*$.

**Remarque :** Chaque opération élémentaire revient à multiplier à gauche par une matrice « simple » : respectivement :

— $T_{i,j}(t)$ « la matrice $I_n$ à laquelle on a ajouté un $t$ en position $i, j$ »

$$\begin{pmatrix} 1 & \dots & t & \\ & \ddots & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

— $\Sigma_{i,j}$ « la matrice obtenue à partir de $I_n$ en permutant les colonnes $i$ et $j$ » :

$$\text{exemple : } \Sigma_{1,n} = \begin{pmatrix} 0 & \dots & & & 1 \\ \vdots & 1 & & & \vdots \\ & & \ddots & & \\ & & & 1 & \\ 1 & & & & 0 \end{pmatrix}$$

— $D_i(\alpha)$ « la matrice obtenue à partir de $I_n$ en remplaçant le $i$ème coefficient diagonal par $\alpha$ :

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & \alpha & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}.$$

**Théorème 2.4.3** *Chaque matrice peut être transformée en une matrice échelonnée par une suite finie d'opérations élémentaires.*

*Démonstration :* Par récurrence sur le nombre de lignes. Soit $A$ une matrice $m \times n$. Soit $j_1$ la première colonne non nulle. Quitte à permuter la première ligne avec une autre, on peut supposer que $a_{1,j_1} \neq 0$. On note $L_1, ..., L_m$ les lignes de $A$. On remplace alors, pour tout $k > 1$, la ligne $L_k$ par $L_k - \frac{a_{k,j_1}}{a_{1,j_1}} L_1$. On obtient alors une matrice de la forme :

$$\begin{pmatrix} 0 & ... & a_{1,j_1} & ... \\ \vdots & & 0 & ... \\ & & \vdots & \\ 0 & & 0 & \end{pmatrix}$$

et on termine par récurrence. *q.e.d.*

**Définition 26** *Le nombre $r$ est le rang des lignes de la matrice.*

**Proposition 2.4.4** *Le rang $r$ est indépendant des transformations effectuées : $r$ est la dimension du sous-espace de $\mathscr{M}_{1,n}(\mathbb{K})$ engendré par les lignes $L_1, ..., L_m$ de la matrice.*

*Démonstration :* En effet, une opération élémentaire ne change pas l'espace vectoriel $\langle L_1, ..., L_m \rangle$ et les lignes non nulles d'une matrice échelonnée sont clairement indépendantes. *q.e.d.*

On peut aussi définir le rang des colonnes de la matrice en utilisant des opérations élémentaires sur les colonnes. Ce rang est égal à la dimension du sous-espace de $\mathscr{M}_{m,1}(\mathbb{K})$ engendré par les colonnes de la matrice.

**Proposition 2.4.5** *Si $A$ est une matrice carrée de taille $n$, si $A$ est de rang $n$, alors $A$ est inversible.*

*Démonstration :* On applique des transformations élémentaires à $A$ jusqu'à obtenir la matrice $I_n$. Si $r = n$, c'est possible. Si on applique les mêmes transformations à $I_n$ on obtient $A^{-1}$. En effet, soit $E_1, ..., E_N$ des matrices « élémentaires » telles que :

$$E_1 ... E_N A = I_n$$

alors :

$$E_1 ... E_N = A^{-1} \ .$$

*q.e.d.*

EXEMPLE : Soit $A := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

On effectue les opérations suivantes :

$$\left(\begin{array}{cc|cc} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array}\right) \overset{L_1 \leftrightarrow L_2}{\rightsquigarrow} \left(\begin{array}{cc|cc} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right)$$

$$\overset{L_1 \leftarrow L_1 - L_2}{\rightsquigarrow} \left(\begin{array}{cc|cc} 1 & 0 & -1 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right)$$

conclusion : $A^{-1} = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$.

Plus généralement, pour une matrice $A \in \mathscr{M}_{m,n}(\mathbb{K})$, le même raisonnement montre qu'il existe $P \in \mathrm{GL}_m(\mathbb{K})$ tel que :

$$PA = \left(\begin{array}{c} I_n \\ \hline 0 \end{array}\right)$$

(en particulier, dans ce cas $n \leq m$).

Si l'on multiplie à gauche par $\left(\begin{array}{c|c} I_n & 0 \end{array}\right)$, on trouve :

$$\left(\begin{array}{c|c} I_n & 0 \end{array}\right) PA = I_n \ .$$

On peut raisonner de même avec les colonnes. En résumé :

**Théorème 2.4.6** *Soit* $A \in \mathscr{M}_{m,n}(\mathbb{K})$*.*

*i) Si le rang des lignes de* $A$ *est* $n$*, alors* $n \leq m$ *et il existe* $P \in \mathrm{GL}_m(\mathbb{K})$ *tel que* $PA = \begin{pmatrix} I_n \\ \hline 0 \end{pmatrix}$ *et il existe* $B \in \mathscr{M}_{n,m}(\mathbb{K})$ *tel que* $BA = I_n$*. On dit que* $A$ *est inversible à gauche.*

*ii) Si le rang des colonnes de* $A$ *est* $m$*, alors* $m \leq n$ *et il existe* $Q \in \mathrm{GL}_n(\mathbb{K})$ *tel que* $AQ = \left( \begin{array}{c|c} I_m & 0 \end{array} \right)$ *et il existe* $B \in \mathscr{M}_{n,m}(\mathbb{K})$ *tel que* $AB = I_m$*. On dit que* $A$ *est inversible à droite.*

### 2.4.3 Égalité entre le rang des lignes et le rang des colonnes

Soit $A \in \mathscr{M}_{m,n}(\mathbb{K})$ une matrice. On rappelle que le rang des lignes de $A$, notons-le $\mathrm{rg}_L(A)$, est la dimension du sous-espace vectoriel de $\mathscr{M}_{1,n}(\mathbb{K})$ engendré par les lignes de $A$. On rappelle que rang des colonnes de $A$, notons-le $\mathrm{rg}_C(A)$, est la dimension du sous-espace vectoriel de $\mathscr{M}_{m,1}(\mathbb{K})$ engendré par les colonnes de $A$.

Alors :

**Théorème 2.4.7**

$$\begin{aligned} &\mathrm{rg}_L(A) \\ &= \min\left\{t \geq 1 \ : \ {}^{\exists}B \in \mathscr{M}_{m,t}(\mathbb{K}),\ {}^{\exists}C \in \mathscr{M}_{t,n}(\mathbb{K}),\ A = BC\right\} \\ &= \mathrm{rg}_C(A)\ . \end{aligned}$$

*On notera* $\mathrm{rg}\,(A)$ *le rang de* $A$ *(des lignes ou des colonnes).*

*En particulier,* $\mathrm{rg}\,(A) \leq \min\{m, n\}$*.*

*Démonstration :*

Montrons par exemple la première égalité (la deuxième se montre de la même façon) :

Notons $r_0$ le minimum des $t$ tels que $A = BC$ pour un certain $B \in \mathscr{M}_{m,t}(\mathbb{K})$ et un certain $C \in \mathscr{M}_{t,n}(\mathbb{K})$.

Soit $r := \mathrm{rg}_L(A)$. Alors, il existe une base $l_1, ..., l_r$ du sous-espace engendré par les lignes de $A$. En particulier, pour toute ligne $L_i$ de $A$,

$$* \ \ L_i = b_{i,1}l_1 + ... + b_{i,r}l_r$$

pour certains coefficients $b_{i,j} \in \mathbb{K}$, $1 \leq i \leq m$, $1 \leq j \leq r$. Soit $B \in \mathscr{M}_{m,r}(\mathbb{K})$ la matrice des $b_{i,j}$ et soit $C \in \mathscr{M}_{r,n}$ la matrice dont les lignes sont $l_1, ..., l_r$. La relation $*$ pour tout $i$, donne : $A = BC$. Donc, $r_0 \leq r$.

D'un autre côté, si $A = BC$ avec $B \in \mathscr{M}_{m,t}(\mathbb{K})$, $C \in \mathscr{M}_{t,n}(\mathbb{K})$. alors pour tout $1 \leq i \leq m$, la ligne $L_i$ de $A$ vérifie :

$$L_i = B_{i,1}l_1 + ..; +B_{i,t}l_t$$

où $l_1, ..., l_t$ sont les lignes de $C$. Donc le sous-espace engendré par les lignes de $A$ est de dimension $\leq t$. Donc $r \leq t$. Et donc, $r \leq r_0$ si on prend $t = r_0$.

En résumé, le rang d'une matrice $A$ est à la fois le rang des lignes de $A$, le rang de ses colonnes et la dimension de son image.

*q.e.d.*

On déduit de cette caractérisation du rang que :

$$\mathrm{rg}\,(AB) \leq \min\{\mathrm{rg}\,A, \mathrm{rg}\,B\}$$

pour toutes matrices $A \in \mathscr{M}_{m,n}(\mathbb{K})$, $B \in \mathscr{M}_{n,p}(\mathbb{K})$.

**Proposition 2.4.8** *Si $A \in \mathscr{M}_{m,n}(\mathbb{K})$ est de rang $r$, il existe $B \in \mathscr{M}_{m,r}(\mathbb{K})$, $C \in \mathscr{M}_{r,n}(\mathbb{K})$ tels que $A = BC$. Dans ce cas, $\mathrm{rg}\,B = r = \mathrm{rg}\,C$. De plus, il existe $P \in \mathrm{GL}_m(\mathbb{K})$, $Q \in \mathrm{GL}_n(\mathbb{K})$ tels que :*

$$PAQ = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right) \quad .$$

*Démonstration :* Si $A = BC$ avec $B \in \mathscr{M}_{m,r}(\mathbb{K})$, $C \in \mathscr{M}_{r,n}(\mathbb{K})$, alors $r = \mathrm{rg}\,A \leq \mathrm{rg}\,B \leq r$ donc $\mathrm{rg}\,B = r$. De même, $\mathrm{rg}\,C = r$. D'après le théorème 2.4.6, il existe donc $P \in \mathrm{GL}_m(\mathbb{K})$, $Q \in \mathrm{GL}_n(\mathbb{K})$ tels que :

$$PB = \left(\begin{array}{c} I_r \\ \hline 0 \end{array}\right) \;,\; CQ = \left(\begin{array}{c|c} I_r & 0 \end{array}\right)$$

D'où :

$$PAQ = PBCQ = \left(\begin{array}{c} I_r \\ \hline 0 \end{array}\right) \left(\begin{array}{c|c} I_r & 0 \end{array}\right) = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$$

*q.e.d.*

Pour terminer voici un critère pratique pour calculer le rang d'une matrice :

**Proposition 2.4.9** *Soit* $A = (a_{i,j})_{\substack{1\leq i\leq m \\ 1\leq j\leq n}} \in \mathscr{M}_{m,n}(\mathbb{K})$*. On dit que* $B$ *est une matrice extraite de* $A$ *si* $B$ *est de la forme :*

$$B = (a_{i,j})_{\substack{i\in I \\ j\in J}}$$

*pour un certain* $I \subseteq \{1, ..., m\}$ *et un certain* $J \subseteq \{1, ..., n\}$*.*

*Le rang de* $A$ *est le plus grand entier* $r$ *tel qu'il existe une matrice* $B$*, extraite de* $A$*, carrée, inversible de taille* $r$*.*

*Exemple :* la matrice

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

n'est pas inversible (*exo*) mais la matrice extraite :

$$\begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix}$$

l'est (*exo*) . Donc $A$ est de rang 2.

*Démonstration :* Soit $B$ une matrice extraite de $A$, carrée, inversible de taille $r$. Supposons pour simplifier que $B = (a_{i,j})_{1\leq i,j\leq r}$. Alors, les $r$ premières lignes de $B$ sont linéairement indépendantes. A fortiori, les $r$ premières lignes de $A$ sont aussi linéairement indépendantes. Donc $\operatorname{rg} A \geq r$. Supposons que $A$ est de rang $R$. Alors il existe $R$ lignes de $A$ qui sont linéairement indépendantes, par exemple les $R$ premières. La matrice

$$(a_{i,j})_{\substack{1\leq i\leq R \\ 1\leq j\leq n}}$$

est donc de rang $R$. Elle admet donc au moins $R$ colonnes indépendantes, par exemple les $R$ premières. Alors la matrice extraite :

$$(a_{i,j})_{1\leq i,j\leq R}$$

est carrée, de taille $R$ et inversible (car de rang $R$). *q.e.d.*

### 2.4.4 Image et noyau d'une matrice

Soit $A \in \mathscr{M}_{m,n}(\mathbb{K})$. On dit que $A$ est *injective* si ses colonnes sont indépendantes. On dit que $A$ est surjective si ses lignes sont indépendantes.

*Remarque :* si $x_1, ..., x_n \in \mathbb{K}$, si on note $C_1, ..., C_n$ les colonnes de $A$, alors :

$$x_1 C_1 + ... + x_n C_n = A. \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

notons :

$$\ker A := \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n \ : \ A. \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0 \right\}$$

c'est un sous-espace de $\mathbb{K}^n$ : c'est le *noyau* de $A$. Alors $A$ est injective $\Leftrightarrow$ $\ker A = 0$.

Notons

$$\mathrm{Im}\, A := \left\{ A. \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n \right\}$$

c'est le sous-espace de $\mathbb{K}^m$ engendré par les colonnes de $A$, on l'appelle *l'image* de $A$. Comme le rang des lignes est aussi le rang des colonnes, les lignes sont indépendantes *i.e.* $A$ est surjective si et seulement si $\mathrm{rg}\, A = m$ $\Leftrightarrow \mathrm{Im}\, A = \mathbb{K}^m$.



**Exercice 23** *Soit* $P \in \mathrm{GL}_m(\mathbb{K})$*. Alors :* $\ker(PA) = \ker A$*.*

**Exercice 24** *Si* $A := \begin{pmatrix} 0 & ... & a_{1,j_1} & ... \\ \vdots & & 0 & ... \\ & & \vdots & \\ 0 & & 0 & \end{pmatrix}$ *est une matrice échelonnée avec* $j_1 < ... < j_r$ *et* $a_{i,j_i} \neq 0$ *pour tout* $1 \leq i \leq r$*, alors l'application linéaire :*

$$\ker A \to \mathbb{K}^{n-r} \ , \ (x_j)_{1 \leq j \leq n} \mapsto (x_j)_{\substack{1 \leq j \leq n \\ j \neq j_1, ..., j_r}}$$

*est un isomorphisme (cf. plus bas le rappel de la notion d'isomorphisme).*

*En particulier,* $\ker A$ *est de dimension* $n - r$*.*

On déduit des deux exercices précédents le

**Théorème 2.4.10 (du rang)**

$$\dim \ker A + \operatorname{rg} A = n$$

*(le nombre de colonnes).*

Pour résumé, on a démontré les équivalences suivantes :

$$A \text{ injective } \Leftrightarrow \operatorname{rg} A = n \Leftrightarrow A \text{ inversible à gauche}$$

$$A \text{ surjective } \Leftrightarrow \operatorname{rg} A = m \Leftrightarrow A \text{ inversible à droite}$$

## 2.5 Lien avec les applications linéaires

### 2.5.1 Matrice associée à une application linéaire

Soit $E$ un $\mathbb{K}-$espace vectoriel.

**Définition 27** *Un endomorphisme de $E$ est une application linéaire $f : E \to E$. On note $\mathrm{End}_{\mathbb{K}}(E)$ ou $\mathcal{L}(E)$ l'ensemble des endomorphismes de $E$.*

Soit $f \in \mathrm{End}_{\mathbb{K}}(E)$. Soit $e_1, ..., e_n$ une base de $E$. Pour tout $1 \leq j \leq n$, il existe $a_{1,j}, ..., a_{n,j} \in \mathbb{K}$ tels que

$$f(e_j) = a_{1,j}e_1 + ... + a_{n,j}e_n$$

en fait, $f$ est entièrement déterminé par ces coefficients : $a_{i,j}$, $1 \leq i, j \leq n$ :

$$\forall v = x_1e_1 + ... + x_ne_n \in E,\ f(v) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_j a_{i,j} e_i \ .$$

autrement dit, si $X := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ est le vecteur « coordonnées de $v$ dans la base $(e)$ » si $Y := \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ est le vecteur « coordonnées de $f(v)$ dans la base $(e)$ » alors :

$$Y = AX$$

où $A$ est la matrice $(a_{i,j})$.

On dit que la matrice $A := (a_{i,j})_{1\leq i,j\leq n}$ est la *matrice de $f$ dans la base* $(e) := e_1, ..., e_n$.

Notation :

$$A := \mathrm{Mat}(f)_{(e)} \ .$$

**Exercice 25** *Soient $f, f' : E \to E$ deux applications linéaires. Soit $(e)$ une base de $E$, alors :*

$$\mathrm{Mat}(f \circ f')_{(e)} = \mathrm{Mat}(f)_{(e)}\mathrm{Mat}(f')_{(e)} \ .$$

EXEMPLE :

— matrices de rotations : soit $R_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ la rotation de centre 0 et d'angle $\theta$ dans le plan. C'est une application linéaire. Dans la base usuelle $e_1, e_2$ de $\mathbb{R}^2$, la matrice de $R_\theta$ est donnée par :

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} .$$

— matrices de la dérivation sur l'espace des polynômes de degré $\leq n$ :

$$\begin{pmatrix} 0 & 1 & 0 & ... & 0 \\ \vdots & \ddots & 2 & & \vdots \\ & & & & \\ & & & & n \\ 0 & ... & & & 0 \end{pmatrix} \text{et} \begin{pmatrix} 0 & 1 & 0 & ... & 0 \\ \vdots & \ddots & 1 & & \vdots \\ & & & & \\ & & & & 1 \\ 0 & ... & & & 0 \end{pmatrix}$$

respectivement dans la base $1, X, ..., X^n$ et dans la base $1, X, ..., \frac{X^n}{n!}$.

### 2.5.2 Théorème du rang

**Théorème 2.5.1** *Soient $E, F$ deux $\mathbb{K}-$espaces vectoriels. On suppose que $f : E \to F$ est linéaire. Alors si $E$ est de dimension finie :*

$$\dim E = \dim \ker f + \mathrm{rg}\, f$$

*où $\mathrm{rg}\, f$ est la dimension de l'image de $f$.*

*Démonstration :* Soit $e_1, ..., e_r$ une base de $\ker f$. On la complète en une base $e_1, ..., e_r, e_{r+1}, ..., e_n$ de $E$. Alors $f(e_{r+1}), ..., f(e_n)$ est une base de $\mathrm{Im}\, f$ (*exo*). *q.e.d.*

**Définition 28** *Un isomorphisme entre deux espaces vectoriels $E$ et $F$ est une application linéaire bijective $f : E \to F$, notation : $E \simeq F$.*

**Corollaire 2.5.1.1 (Miracle de la dimension finie)** *Si $E$ est de dimension finie, si $f : E \to E$ est linéaire, alors $f$ injectif $\Leftrightarrow$ $f$ surjectif $\Leftrightarrow$ $f$ isomorphisme.*

**Remarque : ATTENTION :** il faut le même espace au départ et à l'arrivée (ou au moins deux espaces de même dimension au départ et à l'arrivée).

*Démonstration :*

$$f \text{ injectif } \Rightarrow \ker f = 0$$

$$\Rightarrow \dim f(E) = \dim E$$

$$\Rightarrow f(E) = E$$

*c-à-d* $f$ surjectif. Réciproque :

$$f \text{ surjectif } \Rightarrow f(E) = E$$

$$\Rightarrow \dim \ker f = 0$$

$$\Rightarrow \ker f = 0$$

*i.e.* $f$ injecftif. On utilise que si $V$ est un sous-espace de $U$, alors $V$ est de dimension finie $\leq \dim U$ avec égalité si et seulement si $V = U$. *q.e.d.*

**Versions matricielles :**

Soit $A \in \mathscr{M}_{m,n}(\mathbb{K})$. Alors : $\dim \ker A + \dim \mathrm{Im}\, A = n$.

On dira qu'une matrice $A \in \mathscr{M}_{m,n}(\mathbb{K})$ est injective si

$$\ker A = 0$$

*i.e.*

$$^{\forall}X \in \mathbb{K}^n,\ AX = 0 \Rightarrow X = 0$$

et que $A$ est surjective si :

$$\mathrm{Im}\, A = \mathbb{K}^m$$

*i.e.*

$$^{\forall}Y \in \mathbb{K}^m,\ ^{\exists}X \in \mathbb{K}^n,\ Y = AX\ .$$

Une matrice $A$ est injective $\Leftrightarrow$ $A$ est inversible à gauche *i.e.* :

$$^{\exists}B \in \mathscr{M}_{n,m}(\mathbb{K}),\ BA = I_n\ .$$

En effet, si $BA = I_n$, alors, $AX = 0 \Rightarrow BAX = 0 \Rightarrow I_nX = X = 0$. Réciproquement, si $A$ est injective, le rang de ses lignes est aussi le rang de ses colonnes *i.e.* la dimension de son image. D'après le théorème du rang, ce rang vaut $n$. Donc le sous-espace de $\mathscr{M}_{1,n}(\mathbb{K})(= \mathbb{K}^n)$ engendré par les lignes $L_1, ...L_m$ de $A$ est de dimension $n$. Donc les lignes de $A$ engendrent $\mathscr{M}_{1,n}(\mathbb{K})$. En particulier, si on note $l_1, ..., l_n$ les lignes de la matrice $I_n$ (*i.e.* la base canonique de $\mathscr{M}_{1,n}(\mathbb{K})$), il existe, pour tout $1 \leq i \leq n$, des coefficients $b_{i,1}, ..., b_{i_m} \in \mathbb{K}$ tels que :

$$l_i = b_{i,1}L_1 + ... + b_{i,m}L_m\ .$$

Autrement dit, si on note $B \in \mathscr{M}_{n,m}(\mathbb{K})$ la matrice des $b_{i,j}$, on a :

$$BA = I_n\ .$$

On peut montrer de même (en raisonnant plutôt avec les colonnes) que $A$ est surjective $\Leftrightarrow$ $A$ est inversible à droite *i.e.* :

$$^{\exists}B \in \mathscr{M}_{n,m}(\mathbb{K}),\ AB = I_m\ .$$

Supposons maintenant que $m = n$ et que $A, B \in \mathscr{M}_n(\mathbb{K})$. Alors :

$$AB = I_n \Leftrightarrow BA = I_n$$

*Démonstration :* $AB = I_n \Rightarrow A$ surjective $\Rightarrow A$ injective.
Or :

$$^{\forall}X \in \mathbb{K}^n,\ A(BAX) = (AB)(AX) = A(X) \Rightarrow BAX = X$$

donc $BA = I_n$. *q.e.d.*

**Théorème 2.5.2** *Soit* $A \in \mathscr{M}_{m,n}(\mathbb{K})$. *Alors,*

$$A \text{ injective } \Leftrightarrow \operatorname{rg}(A) = n$$

$$A \text{ surjective } \Leftrightarrow \operatorname{rg}(A) = m$$

*en particulier si* $m = n$, $A$ *injective* $\Leftrightarrow$ $A$ *surjective* $\Leftrightarrow$ $A$ *inversible.*

*Démonstration :* Par exemple : $\operatorname{rg} A = n \Rightarrow \dim ImA = n \Rightarrow \dim\ker A = 0$ et réciproquement si $A$ est injective, alors $A$ est inversible à gauche : il existe $B \in \mathscr{M}_{n,m}(\mathbb{K})$ tel que : $BA = I_n$. Donc $n \geq \operatorname{rg} A \geq \operatorname{rg} BA = n$ et $\operatorname{rg} A = n$. *q.e.d.*

### 2.5.3 Changements de base

— **Interprétation de l'ensemble des bases au moyen des matrices inversibles.**

Soit $e_1, ..., e_n$ une base de $\mathbb{K}^n$. Soit $P \in \mathrm{GL}_n(\mathbb{K})$ une matrice inversible. Les vecteurs :

$$e'_1 = Pe_1, ..., e'_n = Pe_n$$

forment encore une base de $\mathbb{K}^n$. On obtient ainsi toutes les bases de $\mathbb{K}^n$.

En effet, soient $(e')$, $(e)$ deux bases de $\mathbb{K}^n$ (ou de n'importe quel $\mathbb{K}-$espace vectoriel de dimension $n$). Pour tout $j$,

$$e'_j = p_{1,j}e_1 + ... + p_{n,j}e_n$$

pour certains $p_{i,j} \in \mathbb{K}$.

Soit $v \in \mathbb{K}^n$. Si on note $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ ses coordonnées dans la base $(e)$, $\begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}$ ses coordonnées dans la base $(e')$, alors :

$$X = PX'$$

où $P := (p_{i,j})_{1 \leq i,j \leq n}$.

*Démonstration :*

$$v = x_1e_1 + ... + x_ne_n = x'_1e'_1 + ... + x'_ne'_n$$

$$= \sum_{j=1}^{n} x'_j \sum_{i=1}^{n} p_{i,j}e_i$$

$$= \sum_{i=1}^{n} \left( \sum_{j=1}^{n} p_{i,j}x'_j \right) e_i$$

$$\Leftrightarrow {}^{\forall}\, 1 \leq i \leq n,\ x_i = \sum_{j=1}^{n} p_{i,j}x'_j$$

$$\Leftrightarrow X = PX' \ .$$

*q.e.d.*

**Définition 29 (Matrice de passage)** *La matrice $P$ est la matrice de passage de $(e)$ à $(e')$ ; notation :*

$$P_{(e)}^{(e')} \ .$$

**Exercice 26** *$P$ est inversible d'inverse la matrice de passage de $(e')$ à $(e)$.*

— **Formule de changement de base :**

Soit $f$ un endomorphisme de $\mathbb{K}^n$ (ou de n'importe quel $\mathbb{K}-$espace vectoriel de dimension $n$). Soit $A$ la matrice de $f$ dans la base $(e)$, soit $A'$ la matrice de $f$ dans la base $(e')$. Ces deux matrices sont reliées par :

$$A = PA'P^{-1}$$

*Démonstration :* Soit $v \in \mathbb{K}^n$. Soient $X, X', Y, Y'$ respectivement les vecteurs (colonnes) coordonnées de $v$ dans les bases $(e)$ et $(e')$, de $f(v)$ dans les bases $(e)$ et $(e')$.

Alors : $Y = AX$ et $Y' = AX'$ (*exo*). De plus :

$$X = PX',\ Y = PY'$$

$$\Rightarrow PY' = APX'$$

$$\Rightarrow Y' = P^{-1}APX' = A'X'$$

(pour tout $X' \in \mathbb{K}^n$). Donc $P^{-1}AP = A'$.

*q.e.d.*

**Exercice 27**

$$\begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix} \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix}^{-1} = \begin{pmatrix} e^{it} & 0 \\ 0 & e^{-it} \end{pmatrix}$$

# Chapitre 3

# Le déterminant

## 3.1 Dimension 2 et 3

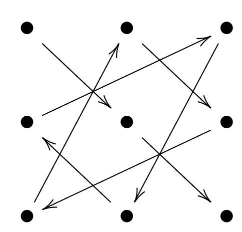
**Définition 30**

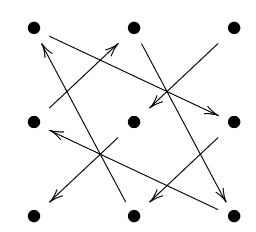
$$\begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix} := a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$$

$$\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix} := a_{1,1}a_{2,2}a_{3,3} + a_{2,1}a_{3,2}a_{1,3} + a_{3,1}a_{1,2}a_{2,3}$$

$$-a_{2,1}a_{2,1}a_{3,3} - a_{1,1}a_{3,2}a_{2,3} - a_{3,1}a_{2,2}a_{1,3}$$

**Moyen mnémotechnique :**





$+$ $-$

**Interprétation géométrique** (sur $\mathbb{R}$) : dét $(A)$ est une aire ou un volume « orienté ».

**Exercice 28** — dét $A \neq 0 \Leftrightarrow A$ *inversible ;* — dét $(AB) =$ dét $A$dét $B$

## 3.2 Déterminant en dimension quelconque

### 3.2.1 Arrangements

Un *arrangement d'ordre* $n$ est une suite

$$\underline{k} := (k_1, ..., k_n)$$

des $n$ entiers $1, ..., n$ dans un ordre quelconque. (Autrement dit une suite $(k_1, ..., k_n)$ où chaque entier $1, ..., n$ apparaît exactement une fois.

*Exemples* : les arrangements d'ordre 2 sont $(1, 2)$ et $(2, 1)$. Les arrangements d'ordre 3 sont $(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1)$. Plus généralement, il y a exactement $n!$ arrangements d'ordre $n$ ($n$ possibilité pour le premier terme, $n - 1$ pour le deuxième, *etc*).

Soit $\underline{k}$ un arrangement. Une *inversion* de $\underline{k}$ est une paire $\{k_i, k_j\}$ telle que $i < j$ et $k_i > k_j$ (« c'est quand un plus grand est à gauche d'un plus petit »).

On note $I(\underline{k})$ l'ensemble des inversions de $\underline{k}$.

On dit qu'un arrangement est *pair* s'il a un nombre pair d'inversions ; on dit qu'il est *impair* s'il a un nombre impair d'inversions. Pour tout arrangement $\underline{k}$ on pose :

$$\epsilon(\underline{k}) := 1 \text{ si } \underline{k} \text{ est un arrangement pair}$$

$$-1 \text{ si } \underline{k} \text{ est un arrangement impair}$$

*Exemple :* voici les inversions et les signatures des 6 arrangements d'ordre 3 :

| $\sigma$ | $I(\sigma)$ <br> $\#I(\sigma)$ | $\epsilon(\sigma)$ |
|---|---|---|
| $(1, 2, 3)$ | $\emptyset$ <br> 0 | 1 |
| $(2, 1, 3)$ | {{1,2}} <br> 1 | $-1$ |
| $(1, 3, 2)$ | {{2,3}} <br> 1 | $-1$ |
| $(2, 3, 1)$ | {{2,3},{1,3}} <br> 2 | 1 |
| $(3, 1, 2)$ | {{3,1},{3,2}} <br> 2 | 1 |
| $(3, 2, 1)$ | {{1,2},{2,3},{1,3}} <br> 3 | $-1$ |

### 3.2.2 Définitions du déterminant

**Définition 31** *Soit* $A = (a_{i,j})_{1 \leq i,j \leq n}$ *une matrice. On note :*

$$\text{dét}\, A := |A| := \sum_{\sigma \text{ arrangement d'ordre n}} \epsilon(\sigma) a_{\sigma(1),1} .... a_{\sigma(n),n}$$

*le déterminant de $A$.*

**Exercice 29** *Pour $n = 2, 3$ on retrouve la définition usuelle.*

**Proposition 3.2.1 (déterminant d'une matrice triangulaire)** *Soit $T = (t_{i,j})_{1\leq i,j\leq n}$ une matrice triangulaire supérieure* i.e. *$t_{i,j} = 0$ si $i > j$. Alors :*

$$\begin{vmatrix} t_{1,1} & \cdots & t_{1,n} \\ 0 & \ddots & \vdots \\ \vdots & \ddots & \\ 0 \cdots & 0 & t_{n,n} \end{vmatrix} = t_{1,1}...t_{n,n}$$

*le produit des coefficients diagonaux. En particulier,*

$$|I_n| = 1$$

.

*Démonstration* : Par définition :

$$|T| = \sum_{\sigma} \epsilon(\sigma) t_{\sigma(1),1}...t_{\sigma(n),n}$$

(somme sur les arrangements $\sigma$ d'ordre $n$)

Or, le produit $t_{\sigma(1),1}...t_{\sigma(n),n}$ est nul sauf si, éventuellement, $\sigma(1) \leq 1, ..., \sigma(n) \leq n$. Cela n'arrive que si $\sigma(1) = 1, ..., \sigma(n) = n$ *c-à-d* si $\sigma = (1, ..., n)$. Donc :

$$|T| = \epsilon((1, 2, ..., n))t_{1,1}...t_{n,n} = t_{1,1}...t_{n,n} \quad .$$

*q.e.d.*

En particulier, $\text{dét}\,(I_n) = 1$.

Cette définition du déterminant et « la seule possible » au sens suivant :

**Théorème 3.2.2** *Il existe une unique application :*

$$D : \mathscr{M}_n(\mathbb{K}) \to \mathbb{K}\,,\ A \mapsto D(A)$$

*i) linéaire en les colonnes de $A$, ii) alternée* i.e. *$D(A) = 0$ si $A$ a deux colonnes identiques, iii) $D(I_n) = 1$.*

*De plus, $D = \text{dét}$ .*

*Démonstration :* Le $i$) signifie que si on note $C_1, ...C_n$ les colonnes d'une matrice $A$. Pour tout $j$, si $C'_j$ est un vecteur colonne, alors, pour tous $\lambda, \mu \in \mathbb{K}$, on a :

$$D(C_1|...|\lambda C_j + \mu C'_j|...|C_n) = \lambda D(C_1|...|C_j|...|C_n) + \mu D(C_1|...|C'_j|...|C_n) \ .$$

*Existence* : Il est clair que dét vérifie i) et iii). Vérifions ii) :

supposons que $A \in \mathscr{M}_n(\mathbb{K})$ a ses colonness $C_i$ et $C_j$ identiques, $i < j$. Pour tout arrangement $\sigma$ d'ordre $n$, posons $\sigma'$ l'arrangement défini par :

$$\sigma'(p) = \begin{cases} \sigma(p) \text{ si } p \neq i, j, \\ \sigma(j) \text{ si } p = i, \\ \sigma(i) \text{ si } p = j. \end{cases}$$

Alors

$$(*) \ \ \epsilon(\sigma) = -\epsilon(\sigma') \ .$$

En effet,

$$(I(\sigma) \cup I(\sigma')) \ \setminus \ (I(\sigma) \cap I(\sigma')) =$$
$$\{\{k_i, k_j\}\} \cup \{\{k_i, k_p\} \ : \ i < p < j\} \cup \{\{k_q, k_j\} \ : \ i < q < j\}$$

qui est un ensemble de cardinal $2(j - i) - 1$ (*exo*) . Donc :

$$|I(\sigma)| + |I(\sigma')| = 2|I(\sigma) \cap I(\sigma')| + 2(j - i) - 1$$
$$\Rightarrow |I(\sigma)| = |I(\sigma')| - 1 \bmod 2$$
$$\Rightarrow \epsilon(\sigma) = -\epsilon(\sigma') \ .$$

On a donc une bijection :

$$\{\sigma \text{ arrangement pair}\} \stackrel{1:1}{\to} \{\sigma \text{ arrangement impair}\}$$

$$\sigma \mapsto \sigma'$$

De plus, comme les colonnes $C_i$ et $C_j$ de la matrice $A$ sont identiques, on a :

$$a_{\sigma(1),1}....a_{\sigma(n),n} = a_{\sigma'(1),1}...a_{\sigma'(n),n}$$

pour tout arrangement $\sigma$.

Donc :

$$\text{dét}\, A = \sum_{\sigma \text{arrangement pair}} a_{\sigma(1),1}....a_{\sigma(n),n} - \sum_{\sigma \text{arrangement impair}} a_{\sigma(1),1}....a_{\sigma(n),n}$$

$$= \sum_{\sigma \text{arrangement pair}} a_{\sigma(1),1} \ldots a_{\sigma(n),n} - \sum_{\sigma \text{arrangement pair}} a_{\sigma'(1),1} \ldots a_{\sigma'(n),n}$$

$$= \sum_{\sigma \text{arrangement pair}} a_{\sigma(1),1} \ldots a_{\sigma(n),n} - a_{\sigma'(1),1} \ldots a_{\sigma'(n),n}$$

$$= 0 \ .$$

*Unicité :* Soit $D$ qui vérifie i), ii) de l'énoncé. Alors, si on note $E_1, ..., E_n$ la base canonique de $\mathscr{M}_{n,1}(\mathbb{K})$, on a :

$$C_j = \sum_{i=1}^{n} a_{i,jE_i}$$

pour toute colonne $C_j$ de $A$ et par linéarité :

$$D(A) = \sum_{i_1,...,i_n=1}^{n} a_{i_1,1} ... a_{i_n,n} D(E_{i_1}|...|E_{i_n}) \ .$$

Or, $D(E_{i_1}|...|E_{i_n}) = 0$ si les $i_1, ..., i_n$ ne sont pas tous distincts. Donc :

$$D(A) = \sum_{(i_1,...,i_n) \text{ arrangment}} D(E_{i_1}|...|E_{i_n}) \ .$$

Il reste à montrer que pour un arrangement $(i_1, ..., i_n)$, $D(E_{i_1}|...|E_{i_n}) = \epsilon(i_1, ..., i_n) D(I_n)$. On le démontre par récurrence sur $k \geq 1$ tel que :

$$i_{k-1} > i_k < ... < i_n \ .$$

Si $k = 1$, c'est évident car alors, $i_1 = 1, ..., i_n = n$. Si $k > 1$, on échange $i_{k-1}$ et $i_k$ : on obtient un arrangement : $(i'_1, ..., i'_n)$ où $i'_j := i_j$ si $j \neq k, k+1$, $i'_k := i_{k-1}$ et $i'_{k-1} := i_k$. Comme :

$$i'_{k-1} < ... < i'_n$$

on a par hypothèse de récurrence :

$$D(E_{i'_1}|...|E_{i'_n}) = \epsilon(i'_1, ..., i'_n) D(I_n) \ .$$

Or, d'après (*), on a :

$$\epsilon(i'_1, ..., i'_n) = -\epsilon(i_1, ..., i_n) \ .$$

De plus, on a :

$$D(E_{i_1}|...|E_{i_{k-1}} + E_{i_k}|E_{i_{k-1}} + E_{i_k}|...|E_{i_n}) = 0$$

$$\Leftrightarrow D(E_{i_1}|...|E_{i_{k-1}}|E_{i_{k-1}}|...|E_{i_n}) + D(E_{i_1}|...|E_{i_{k-1}}|E_{i_k}|...|E_{i_n})$$
$$+D(E_{i_1}|...|E_{i_k}|E_{i_{k-1}}|...|E_{i_n}) + D(E_{i_1}|...|E_{i_k}|E_{i_k}|...|E_{i_n}) = 0$$
$$\Leftrightarrow D(E_{i_1}|...|E_{i_{k-1}}|E_{i_k}|...|E_{i_n}) + D(E_{i_1}|...|E_{i_k}|E_{i_{k-1}}|...|E_{i_n}) = 0$$
$$\Leftrightarrow D(E_{i_1}|...|E_{i_n}) = -D(E_{i'_1}|...|E_{i'_n}) \ .$$

Conclusion : $D(E_{i_1}|...|E_{i_n}) = \epsilon(i_1, ..., i_n)D(I_n)$. *q.e.d.*

On a en fait démontrer le résultat suivant :

**Théorème 3.2.3** *Soit* $D : \mathscr{M}_n(\mathbb{K}) \to \mathbb{K}$ *une application* $n-$*linéaire et alternée en les colonnes (* i.e. *qui vérifie i) et ii) du théorème précédent), alors :*

$$D(A) = \text{dét}\, A D(I_n) \ .$$

## Déterminant de la transposée

Si $A \in \mathscr{M}_{m,n}(\mathbb{K})$, on note ${}^tA \in \mathscr{M}_{n,m}(\mathbb{K})$ la matrice de coefficients :

$$({}^tA)_{i,j} := A_{j,i}$$

pour tous $1 \leq i \leq m$, $1 \leq j \leq n$.

**Théorème 3.2.4** *Soit* $A \in \mathscr{M}_n(\mathbb{K})$. *Alors,* $\text{dét}\,({}^tA) = \text{dét}\, A$.

**Corollaire 3.2.4.1** *Dans les théorèmes 3.2.2 et 3.2.3, on peut remplacer « colonne » par « ligne » .*

*Démonstration* : Si $\sigma$ est un arrangement d'ordre $n$, on note $\sigma^{-1} := (l_1, ..., l_n)$ l'arrangementy d'ordre $n$ tel que $\sigma_{l_i} = i$ pour tout $i$. Si $1 \leq i \neq j \leq n$, alors $\{\sigma_i, \sigma_j\}$ est une inversion de $\sigma$ si et seulement si $\{i, j\}$ est une inversion de $\sigma^{-1}$ (*exo*) . En particulier, $\epsilon(\sigma) = \epsilon(\sigma^{-1})$ pour tout arrangement $\sigma$.

Or, on a :

$$a_{\sigma(1),1}...a_{\sigma(n),n} = a_{\sigma(\sigma^{-1}(1)),\sigma^{-1}(1)}...a_{\sigma(\sigma^{-1}(n)),\sigma^{-1}(n)}$$
$$= a_{1,\sigma^{-1}(1)}...a_{n,\sigma^{-1}(n)} \ .$$

Donc :

$$\text{dét}\, A = \sum_\sigma \epsilon(\sigma) a_{\sigma(1),1}...a_{\sigma(n),n}$$
$$= \sum_\sigma \epsilon(\sigma) a_{1,\sigma^{-1}(1)}...a_{n,\sigma^{-1}(n)}$$

$$= \sum_\sigma \epsilon(\sigma^{-1}) a_{1,\sigma(1)} ... a_{n,\sigma(n)}$$

$$= \sum_\sigma \epsilon(\sigma) a_{1,\sigma(1)} ... a_{n,\sigma(n)}$$

$$= \text{dét}\,({}^t A) \ .$$

*q.e.d.*

**Conséquences :**

**Théorème 3.2.5 (déterminant du produit)** *Soient* $B \in \mathscr{M}_n(\mathbb{K})$ *:*

$$\text{dét}\,(AB) = \text{dét}\, A \text{dét}\, B \ .$$

*Démonstration :* En effet, si $A$ est fixée, l'application :

$$F \ : \ B \mapsto \text{dét}\,(AB)$$

est $n-$linéaire alternée en les colonnes de $B$. Donc :

$$\forall B \in \mathscr{M}_n(\mathbb{K}),\ F(B) = \text{dét}\, B F(I_n)$$

$$= \text{dét}\, A \text{dét}\, B \ .$$

*q.e.d.*

EXEMPLE : Pour les matrices de Pascal de la page 29, on trouve :

$$\text{dét}\, P = \text{dét}\, T_- T^+ = 1 \ .$$

**Proposition 3.2.6 (déterminant des matrices triangulaires par blocs)** *Si* $A \in \mathscr{M}_m(\mathbb{K})$, $B \in \mathscr{M}_{m,n}(\mathbb{K})$, $D \in \mathscr{M}_n(\mathbb{K})$, *alors :*

$$\left| \begin{array}{c|c} A & B \\ \hline 0 & D \end{array} \right| = \text{dét}\, A \text{dét}\, D \ .$$

*Démonstration :* Fixons $A$. L'application :

$$D \mapsto \left| \begin{array}{c|c} A & B \\ \hline 0 & D \end{array} \right|$$

est $n-$linéaire alternée en les lignes de $D$ donc :

$$\left|\begin{array}{c|c} A & B \\ \hline 0 & D \end{array}\right| = \text{dét}\, D \left|\begin{array}{c|c} A & B \\ \hline 0 & I_n \end{array}\right|$$

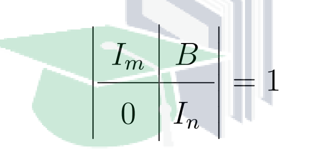
Ensuite $B$ étant fixé, l'application :

$$A \mapsto \left|\begin{array}{c|c} A & B \\ \hline 0 & I_n \end{array}\right|$$

est $n-$linéaire alternée en les colonnes de $A$ donc :

$$\left|\begin{array}{c|c} A & B \\ \hline 0 & I_n \end{array}\right| = \text{dét}\, A \left|\begin{array}{c|c} I_m & B \\ \hline 0 & I_n \end{array}\right|$$

enfin, on sait calculer le déterminant d'une matrice triangulaire supérieure (on fait le produit des termes diagonaux) :



$$\left|\begin{array}{c|c} I_m & B \\ \hline 0 & I_n \end{array}\right| = 1$$



*q.e.d.*

## 3.3 Règle de Cramer

Notation : Soit $A$ une matrice $n \times n$. On note $A^{i,j}$ la matrice obtenue en biffant † la ligne $i$ et la colonne $j$ de $A$.

On peut calculer un déterminant $n \times n$ si on sait calculer un déterminant $(n-1) \times (n-1)$ :

**Proposition 3.3.1 (Développement par rapport à une ligne ou une colonne)** *Soit $A$ une matrice $n \times n$. Alors :*

$$^{\forall}1 \leq j \leq n,\ \text{dét}\, A = \sum_{i=1}^{n} (-1)^{i+j} a_{i,j} |A^{i,j}|$$

†. BIFFER, verbe transitif :
Barrer, annuler d'un trait de plume ce qui est écrit. *Ses manuscrits étaient biffés, rebiffés, raturés, grattés, chargés* (CHAMPFLEURY, *Les Souffrances du professeur Delteil*, 1855, p. 176)

$$\forall 1 \leq i \leq n, \text{ dét } A = \sum_{j=1}^{n} (-1)^{i+j} a_{i,j} |A^{i,j}| \ .$$

*Démonstration :* Par $n-$linéarité du déterminant selon les colonnes, comme on a :

$$A = \sum_{i=1}^{n} a_{i,j} \begin{pmatrix} a_{1,1} & \dots & \overset{\overset{j}{|}}{0} & \dots & a_{1,n} \\ \vdots & & \vdots & & \vdots \\ a_{i,1} & & 1 & & a_{i,n} \\ \vdots & & \vdots & & \vdots \\ a_{n,1} & \dots & 0 & \dots & a_{n,n} \end{pmatrix},$$

on a :

$$\text{dét } A = \sum_{i=1}^{n} a_{i,j} \begin{vmatrix} a_{1,1} & \dots & \overset{\overset{j}{|}}{0} & \dots & a_{1,n} \\ \vdots & & \vdots & & \vdots \\ a_{i,1} & & 1 & & a_{i,n} \\ \vdots & & \vdots & & \vdots \\ a_{n,1} & \dots & 0 & \dots & a_{n,n} \end{vmatrix}.$$

Or en échangeant la colonne $j$ avec la colonne $j-1$ puis la colonne $j-1$ avec la colonne $j-2$, etc, on trouve :

$$\begin{vmatrix} a_{1,1} & \dots & 0 & \dots & a_{1,n} \\ \vdots & & \vdots & & \vdots \\ a_{i,1} & & 1 & & a_{i,n} \\ \vdots & & \vdots & & \vdots \\ a_{n,1} & & 0 & & a_{n,n} \end{vmatrix} = (-1)^{j-1} \begin{vmatrix} 0 & a_{1,1} & \dots & a_{1,n} \\ \vdots & \vdots & & \vdots \\ 1 & a_{i,1} & \dots & a_{i,n} \\ \vdots & \vdots & & \vdots \\ 0 & a_{n,1} & \dots & a_{n,n} \end{vmatrix}$$

ensuite, en échangeant la ligne $i$ avec la ligne $i-1$ puis la ligne $i-1$ avec la ligne $i-2$, etc, on obtient :

$$\begin{vmatrix} a_{1,1} & \dots & 0 & \dots & a_{1,n} \\ \vdots & & \vdots & & \vdots \\ a_{i,1} & & 1 & & a_{i,n} \\ \vdots & & \vdots & & \vdots \\ a_{n,1} & & 0 & & a_{n,n} \end{vmatrix} = (-1)^{j-1}(-1)^{i-1} \begin{vmatrix} 1 & a_{i,1} & \dots & a_{i,n} \\ 0 & a_{1,1} & \dots & a_{1,n} \\ \vdots & \vdots & & \vdots \\ 0 & a_{n,1} & \dots & a_{n,n} \end{vmatrix}$$

$$= (-1)^{i+j}|A^{i,j}| \ .$$

Et on démontre de même la formule de développement par rapport à la ligne $i$. *q.e.d.*

EXEMPLE :

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} = \begin{vmatrix} 5 & 6 \\ 8 & 9 \end{vmatrix} - 4\begin{vmatrix} 2 & 3 \\ 8 & 9 \end{vmatrix} + 7\begin{vmatrix} 2 & 3 \\ 5 & 6 \end{vmatrix} = 0 \ .$$

**Proposition 3.3.2 (formule de Cramer pour les solutions des systèmes linéaires)** *Si :*

$$\begin{cases} a_{1,1}x_1 + ... + a_{n,1}x_n & = & y_1 \\ & ... & \\ a_{n,1}x_1 + ... + a_{n,n}x_n & = & y_n \end{cases}$$

*alors,* $\text{dét}\, A x_k = \text{dét}\, A_k$ *où* $A_k$ *est la matrice obtenue en remplaçant la* $k-$*ième colonne de* $A$ *par la colonne* $\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$.

*Démonstration :* On développe par rapport à la $k-$ième colonne :

$$\text{dét}\, A_k = \sum_{i=1}^{n} y_i(-1)^{i+k}|A^{i,k}|$$

(on remplace les $y_i$ par leur expression en fonction des $x_j$) :

$$\text{dét}\, A_k = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{i,j}x_j(-1)^{i+k}|A^{i,k}|$$

$$= \sum_{j=1}^{n}\left(\sum_{i=1}^{n} a_{i,j}(-1)^{i+k}|A^{i,k}|\right) x_j \ .$$

Or :

$$\sum_{i=1}^{n} a_{i,j}(-1)^{i+k}|A^{i,k}|$$

est le déterminant de la matrice obtenue en remplaçant la colonne $k$ de la matrice $A$ par la colonne $j$ (*exo*) . Donc :

$$\sum_{i=1}^{n} a_{i,j}(-1)^{i+k}|A^{i,k}| = \begin{cases} 0 \text{ si } k \neq j \\ \text{dét}\, A \text{ sinon} \end{cases} .$$

*q.e.d.*

**Remarque :** Si $\text{dét}\, A \neq 0$, alors $A$ inversible. En effet, dans ce cas, les formules de Cramer montrent que l'on peut inverser le système défini par $A$.

Plus précisément, on peut décrire la matrice inverse de $A$ si $\text{dét}\, A \neq 0$.

**Définition 32 (Comatrice)** *Soit $A$ une matrice $n \times n$, sa comatrice, notée* $\text{com}(A)$ *ou $\widetilde{A}$ est la matrice $n \times n$ dont le $(i, j)-$ième coefficient est :*

$$\widetilde{A}_{i,j} = (-1)^{i+j}|A^{i,j}| \ .$$

**Corollaire 3.3.2.1** *Pour toute matrice $A$ de taille $n \times n$ :*

$${}^t\widetilde{A}A = A{}^t\widetilde{A} = \text{dét}\, AI_n$$

*Démonstration :* En effet, le $(i, j)-$ème coefficient de ${}^t\widetilde{A}A$ est donnée par la formule :

$$\sum_{k=1}^{n}(-1)^{i+k}a_{k,j}|A^{k,i}|$$

qui est le déterminant de la matrice obtenue en remplaçant, dans la matrice $A$, la colonne $i$ par la colonne $j$. Donc :

$$({}^t\widetilde{A}A)_{i,j} = \sum_{k=1}^{n}(-1)^{i+k}a_{k,j}|A^{k,i}|$$

$$= \begin{cases} 0 \text{ si } i \neq j \\ \text{dét}\, A \text{ si } i = j \end{cases} .$$

*q.e.d.*

**Remarque :** Cette formule reste vraie si $\mathbb{K}$ est remplacé par un anneau commutatif (p. ex : $\mathbb{Z}, \mathbb{K}[T]$).

Exemple :

— Si $ad - bc \neq 0$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

— Si $A$ est une matrice $3 \times 3$ et si $|A| \neq 0$, alors :

$$A^{-1} = \frac{1}{|A|} \begin{pmatrix} |A^{1,1}| & -|A^{2,1}| & |A^{3,1}| \\ -|A^{1,2}| & |A^{2,2}| & -|A^{3,2}| \\ |A^{1,3}| & -|A^{2,3}| & |A^{3,3}| \end{pmatrix} .$$

**Théorème 3.3.3** *$A$ est inversible $\Leftrightarrow$ dét $A \neq 0$ et l'inverse est donné par :*

$$A^{-1} = \frac{1}{\text{dét}\, A} {}^t\widetilde{A} = \frac{1}{\text{dét}\, A} \left( \pm |A^{j,i}| \right)$$

Terminons ce chapitre par quelques déterminants remarquables :

**Exercice 30** *Déterminant de Vandermonde. C'est le déterminant $(n+1) \times (n+1)$ suivant :*

$$V(x_0, ..., x_n) = \begin{vmatrix} 1 & \cdots & 1 \\ x_0 & \cdots & x_n \\ \vdots & & \vdots \\ x_0^n & \cdots & x_n^n \end{vmatrix} .$$

*On a : $V(x_1, ..., x_n) = \prod_{0 \leq i < j \leq n} (x_j - x_i)$.*

*Indication : on peut raisonner par récurrence et remarquer que : $V(x_0, ..., x_n)$ est un polynôme de degré $\leq n$ en $x_n$, de coefficient dominant $V(x_0, ..., x_{n-1})$ qui s'annule lorsque $x_n = x_0, ..., x_{n-1}$ ; donc : $V(x_0, ..., x_n) = V(x_0, ..., x_{n-1})(x_n - x_0)...(x_n - x_{n-1})$.*

*Conséquence : Si $x_1, ..., x_n \in \mathbb{C}$, alors :*

$$\begin{cases} x_1 + ... + x_n = 0 \\ \vdots \\ x_1^n + ... + x_n^n = 0 \end{cases} \Rightarrow x_1 = ... = x_n = 0$$

*(ce système n'est pas linéaire).*

**Exercice 31** *Montrer que le déterminant $n \times n$ suivant :*

$$\begin{vmatrix} 1 & -1 & 0 & \cdots & 0 \\ 1 & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & -1 \\ 0 & \cdots & 0 & 1 & 1 \end{vmatrix}$$

*est le $n+1-$ième nombre de Fibonacci $f_{n+1}$ (cf. p. 31).*

Enfin voici une autre façon de calculer un déterminant $3 \times 3$ :

**Exercice 32** *Soit $A$ une matrice $3 \times 3$. Alors si $a_{2,2} \neq 0$ :*

$$|A| = \frac{\begin{vmatrix} \begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix} & \begin{vmatrix} a_{1,2} & a_{1,3} \\ a_{2,2} & a_{2,3} \end{vmatrix} \\ \begin{vmatrix} a_{2,1} & a_{2,2} \\ a_{3,1} & a_{3,2} \end{vmatrix} & \begin{vmatrix} a_{2,2} & a_{2,3} \\ a_{3,2} & a_{3,3} \end{vmatrix} \end{vmatrix}}{a_{2,2}}$$



## 3.4 Déterminant d'un endomorphisme

Soit $E$ un $\mathbb{K}-$espace vectoriel de dimension finie. Soit $u$ un endomorphisme de $E$. Le déterminant :

$$\text{dét}\left(\text{Mat}(u)_{(e)}\right)$$

est indépendant de la base $(e)$ de $E$ choisie.

En effet, les matrices de $u$ dans 2 bases différentes sont semblables et par *multiplicativité* du déterminant :

$$\begin{aligned} \forall A \in \mathscr{M}_n(\mathbb{K}), \forall P \in \text{GL}_n(\mathbb{K}), \text{dét}\,(PAP^{-1}) &= \text{dét}\,P \text{dét}\,A \text{dét}\,(P^{-1}) \\ &= \text{dét}\,A \text{dét}\,P \text{dét}\,P^{-1} \\ &= \text{dét}\,A \end{aligned}$$

(leurs déterminants sont égaux).

On peut donc définir le déterminant de $u$ :

**Définition 33 (déterminant d'un endomorphisme)**

$$\text{dét}\, u := \text{dét}\, A$$

*où $A$ est la matrice de $u$ dans une base quelconque de $E$.*

**Remarque :** [(s) importantes]
— $\text{dét}\, \text{Id}_E = 1$ et pour tous $u, v$ endomorphismes de $E$,

$$\text{dét}\, (u \circ v) = \text{dét}\, u \text{dét}\, v$$

— $u$ est un isomorphisme $\Leftrightarrow$ $\text{dét}\, u \neq 0 \Leftrightarrow \text{Mat}(u)_{(e)}$ inversible (pour toute base $(e)$ de $E$.

En effet, $u$ est un isomorphisme $\Leftrightarrow$ $\text{Mat}(u)_{(e)}$ est inversible (quelle que soit la base $(e)$ de $E$ choisie (*exo*) .

# Chapitre 4

# Valeurs propres, vecteurs propres

Dans ce chapitre $E$ est un $\mathbb{K}-$espace vectoriel.

## 4.1 Sous-espaces invariants

**Définition 34 (sous-espace invariant)** *Soit $u$ un endomorphisme de $E$. On dit qu'un sous-$K-$espace vectoriel $F$ de $E$ est invariant, ou stable, par $u$ si :*

$$^{\forall} x \in F,\ u(x) \in F\ .$$

*On note alors $u|_F : F \to F,\ x \in F \mapsto u(x) \in F$ la restriction de $u$ à $F$. L'application $u|_F$ est un endomorphisme de $F$.*

**Effet sur les matrices :**

Supposons que $E$ est de dimension $n$, que $u$ est un endomorphisme de $E$, que $F$ est un sous-espace de $E$ invariant par $u$. Alors si :

$$e_1, ..., e_k$$

est une base de $F$, on peut la compléter en une base de $E$ :

$$(e) = e_1, ..., e_k, e_{k+1}, ..., e_n\ .$$

La matrice de $u$ dans la base $(e)$ est *triangulaire* par blocs :

$$\mathrm{Mat}(u)_{(e)} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,k} & b_{1,1} & \cdots & b_{1,n-k} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{k,1} & \cdots & a_{k,k} & b_{k,1} & \cdots & b_{k,n-k} \\ 0 & \text{—} & 0 & d_{1,1} & \cdots & d_{1,n-k} \\ | & & | & \vdots & & \vdots \\ 0 & \text{—} & 0 & d_{n-k,1} & \cdots & d_{n-k,n-k} \end{pmatrix}$$

où $A := (a_{i,j})_{1\leq i,j\leq k} \in \mathscr{M}_k(\mathbb{K})$ est la matrice de $u|_F$ dans la base $e_1, ..., e_k$ de $F$, $B := (b_{i,j})_{\substack{1\leq i\leq n-k \\ 1\leq j\leq n-k}} \in \mathscr{M}_{k,n-k}(\mathbb{K})$, $D := (d_{i,j})_{1\leq i,j\leq n-k} \in \mathscr{M}_{n-k}(\mathbb{K})$.

**Remarque :** si le sous-epace :

$$G := \langle e_{k+1}, ..., e_n\rangle$$

est aussi stable par $u$, le bloc rectangulaire $B$ est nul et :

$$\mathrm{Mat}(u)_{(e)} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,k} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{k,1} & \cdots & a_{k,k} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & d_{1,1} & \cdots & d_{1,n-k} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & d_{n-k,1} & \cdots & d_{n-k,n-k} \end{pmatrix}$$

qui est une matrice *diagonale* par blocs.

Exemple : Soit $e_1, e_2, e_3$ la base canonique de $\mathbb{R}^3$. Soit $r_\theta$ la rotation d'axe $e_3$ et d'angle $\theta$. L'endomorphisme $r_\theta$ de $\mathbb{R}^3$ laisse invariants les sous-espaces :

$$\langle e_1, e_2\rangle \text{ et } \langle e_3\rangle$$

et sa matrice dans la base $e_1, e_2, e_3$ est la matrice :

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} .$$

Les droites invariantes sont appelées *droites propres*, ce sont les droites engendrées par les vecteurs propres.

## 4.2 Vecteurs propres

**Définition 35 (vecteurs,valeurs propres, spectre)** *Soit $u$ un endomorphisme de $E$. Un vecteur propre de $u$ est un vecteur* **non nul** $x \in E \setminus \{0\}$ *tel que :*

$$u(x) = \lambda x$$

*pour un certain scalaire $\lambda \in \mathbb{K}$. On dit que $\lambda$ est la valeur propre de $u$ associée au vecteur propre $x$. On dit aussi que $x$ est un vecteur propre associé à la valeur propre $\lambda$.*

*Le spectre de $u$ est l'ensemble des valeurs propres de $u$. Notation :* $\mathrm{Sp}_{\mathbb{K}}(u)$ *(ou* $\mathrm{Sp}(u)$*).*

**Version matricielle** :

Soit $A \in \mathscr{M}_n(\mathbb{K})$. Un *vecteur propre* de $A$ est un vecteur **non nul** $X \in \mathbb{K}^n \setminus \{0\}$ tel que :

$$AX = \lambda X$$

pour un certain scalaire $\lambda \in \mathbb{K}$. On dit que $\lambda$ est la *valeur propre* de $A$ associée au vecteur propre $X$. On dit aussi que $X$ est un vecteur propre associé à la valeur propre $\lambda$.

Le spectre de $A$ est l'ensemble des valeurs propres de $A$. Notation : $\mathrm{Sp}_{\mathbb{K}}(A)$ (ou $\mathrm{Sp}(A)$ si le corps où l'on se place est évident).

EXEMPLE : [s]

— soient $E = \mathbb{R}^3$, $u = r_\theta$ la rotation d'axe $e_3$ et d'angle $\theta$. Alors $r_\theta(e_3) = e_3$. Donc $e_3$ est un vecteur propre de $r_\theta$ ; la valeur propre associée est 1.

— Soit $E = \mathbb{C}[X]_{\leq n}$ l'espace des polynômes complexes de degré $\leq n$. Soit $u = \partial : E \to E$, $P(X) \mapsto P'(X)$. Pour des raisons de degré,

$$P' = \lambda P \Rightarrow \lambda = 0 \text{ et } P \text{ constant}$$

de plus, tout polynôme constant non nul est un vecteur propre de $\partial$ de valeur propre associée 0 ; donc $\mathrm{Sp}(\partial) = \{0\}$.

— (Cet exemple est en dimension infinie) Soit $E = \mathscr{C}^\infty(\mathbb{R})$ l'espace des fonctions infiniment dérivables de $\mathbb{R}$ dans $\mathbb{R}$. Soit $u = \partial : E \to E$, $f \mapsto f'$.

Pour tout $\lambda \in \mathbb{R}$, posons

$$e_\lambda : \mathbb{R} \to \mathbb{R},\ x \mapsto e^{\lambda x} \ .$$

On a : $e'_\lambda = \lambda e_\lambda$ donc chaque fonction $e_\lambda$ est un vecteur propre de $\partial$ de valeur propre associée $\lambda$.

— Soit $A := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Le réel $\alpha := \frac{1+\sqrt{5}}{2}$ est une valeur propre de $A$. En effet :

$$A.\begin{pmatrix} 1 \\ \alpha \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ \alpha \end{pmatrix}$$

(*exo*)

— Soit $A := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Le complexe $j := -\frac{1}{2} + i\frac{\sqrt{3}}{2} = e^{i\frac{2\pi}{3}}$ est une valeur propre de $A$. En effet :

$$A\begin{pmatrix}1\\j\end{pmatrix}=j\begin{pmatrix}1\\j\end{pmatrix}$$

(*exo*)

« Comment trouver les valeurs propres d'un endomorphisme ou d'une matrice parmi tous les éléments de $\mathbb{K}$ ? »

## 4.3 Polynôme caractéristique

**Proposition 4.3.1** *Soient $A \in \mathscr{M}_n(\mathbb{K})$ et $\lambda \in \mathbb{K}$. Alors :*

$$\lambda \text{ est une valeur propre de } A \Leftrightarrow \text{dét}\,(A-\lambda I_n)=0\ .$$

*Démonstration* : $\lambda$ n'est pas une valeur propre de $A$

$$\Leftrightarrow {}^\forall X \in \mathbb{K}^n \setminus \{0\},\ AX \neq \lambda X\, i.e.\ (A-\lambda I_n)X \neq 0$$

$$\Leftrightarrow \ker(A-\lambda I_n)=\{0\}$$

$$\Leftrightarrow A-\lambda I_n \text{ injective}$$

$$\Leftrightarrow A-\lambda I_n \text{ inversible}$$

$$\Leftrightarrow \text{dét}\,(A-\lambda I_n)\neq 0\ .$$

*q.e.d.*

**Définition 36 (polynôme caractéristique)** *Soit $A \in \mathscr{M}_n(\mathbb{K})$. Le polynôme caractéristique de $A$ est : $\chi_A(X) := \text{dét}\,(XI_n - A)$ .*

**Remarque :** [s] — La matrice $XI_n - A$ est à coefficients dans $\mathbb{K}[X]$ donc son déterminant $\chi_A(X) \in \mathbb{K}[X]$.

— Pour tout $\lambda \in \mathbb{K}$, dét $(A-\lambda I_n) = (-1)^n\chi_A(\lambda)$.

EXEMPLE : [s]

— Si $n = 2$ :

$${}^\forall A = \begin{pmatrix} a & b \\ c & d\end{pmatrix},\ \chi_A(X) = X^2-(a+d)X+(ad-bc)$$

$$= X^2 - (\text{tr}A)X + \text{dét}\,A$$

où $\mathrm{tr}A := a + d$.

— Si $n = 3$,

$$^\forall A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}, \ \chi_A(X) = X^3 - (\mathrm{tr}A)X^2 + s_2X - \text{dét}\, A$$

où $\mathrm{tr}A := a_{1,1} + a_{2,2} + a_{3,3}$ et :

$$s_2 := \begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix} + \begin{vmatrix} a_{2,2} & a_{2,3} \\ a_{3,2} & a_{3,3} \end{vmatrix} + \begin{vmatrix} a_{1,1} & a_{1,3} \\ a_{3,1} & a_{3,3} \end{vmatrix}$$

(c'est la trace de la comatrice de $A$).

— $n$ quelconque :

$$^\forall A \in \mathscr{M}_n(\mathbb{K}),\ \chi_A(X) = X^n - s_1X^{n-1} + ... + (-1)^n s_n$$

où pour tout $1 \leq d \leq n$, le coefficient devant $(-1)^d X^{n-d}$ est :

$$s_d := \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I|=d}} |A_I|$$

avec pour tout $I = \{k_1, ..., k_d\}$, tel que $k_1 < ... < k_d$,

$$A_I := \begin{pmatrix} a_{k_1,k_1} & \cdots & a_{k_1,k_d} \\ \vdots & & \vdots \\ a_{k_d,k_1} & \cdots & a_{k_d,k_d} \end{pmatrix} \in \mathscr{M}_d(\mathbb{K})$$

(c'est la matrice obtenue en ne gardant de $A$ que les lignes et les colonnes $k_1, , , k_d$).

*Démonstration :* On pose $P(X_1, ..., X_n) := \begin{vmatrix} X_1 - a_{1,1} & -a_{1,2} & \ldots & \\ -a_{2,1} & X_2 - a_{2,2} & \ldots & \\ \vdots & & \ddots & \\ & & & X_n - a_{n,n} \end{vmatrix}$.

C'est un polynôme en les variables $X_1, ..., X_n$ et à coefficients dans $\mathbb{K}$. On montre par récurrence sur $k$ que pour $1 \leq i_1 < ... < i_k \leq n$, le coefficient devant le monôme $X_{i_1}...X_{i_k}$ est :

$$(-1)^{n-k}\text{dét}\, A^I$$

où $I := \{i_1, ..., i_k\}$ et $A^I$ est la matrice obtenue à partir de $A$ en retirant les lignes et les colonnes $i_1, ..., i_k$ (il suffit de développer par rapport à la ligne $i_1$ puis $i_2, ...$).

En particulier,

$$P(X, ...X) = \chi_A(X) = \sum_{k=0}^{n} (-1)^{n-k} \Big( \sum_{1 \le i_1 < ... < i_k} |A^{\{i_1,...,i_k\}}| \Big) X^k$$

$$= \sum_{k=0}^{n} (-1)^k \Big( \sum_{1 \le i_1 < ... < i_k} |A_{\{i_1,...,i_k\}}| \Big) X^{n-k} \ .$$

*q.e.d.*

**À retenir :** le polynôme $\chi_A(X)$ est unitaire† de degré $n$ et :

$$s_1 = \sum_{i=1}^n a_{i,i} =: \mathrm{tr} A$$

$$s_2 = \sum_{1 \le i < j \le n} \begin{vmatrix} a_{i,i} & a_{i,j} \\ a_{j,i} & a_{j,j} \end{vmatrix}$$

$$s_n = \text{dét}\, A \ .$$

**Définition 37 (deux définitions équivalentes de la trace)** *Soit $A \in \mathscr{M}_n(\mathbb{K})$. On définit la trace de $A$ par :*

$$\mathrm{tr} A := - \text{ le coefficient devant } X^{n-1} \text{ dans } \chi_A(X)$$

*ou par :*

$$\mathrm{tr} A := \text{ la somme des coefficients diagonaux de } A.$$

**Théorème 4.3.2 (polynôme caractéristique d'un produit)** *Soient $m, n$ des entiers $\geq 1$. Si $A \in \mathscr{M}_{m,n}(\mathbb{K})$ et $B \in \mathscr{M}_{n,m}(\mathbb{K})$, alors :*

$$AB \in \mathscr{M}_m(\mathbb{K}) \text{ et } BA \in \mathscr{M}_n(\mathbb{K})$$

*et :*

$$X^n \chi_{AB}(X) = X^m \chi_{BA}(X)$$

*dans $\mathbb{K}[X]$.*

*En particulier, si $m = n$ alors :*

$$\chi_{AB}(X) = \chi_{BA}(X) \ .$$

†. *c-à-d* son coefficient de plus haut degré est 1.

*Démonstration :* On pose :

$$M := \left(\begin{array}{c|c} XI_m & -A \\ \hline 0 & I_n \end{array}\right) \text{ et } N := \left(\begin{array}{c|c} I_m & A \\ \hline B & XI_n \end{array}\right) \in \mathscr{M}_{m+n}(\mathbb{K}) \ .$$

On a alors :

$$MN = \left(\begin{array}{c|c} XI_m - AB & 0 \\ \hline XB & XI_n \end{array}\right)$$

donc :

$$\begin{aligned} \text{dét}\,(MN) &= \text{dét}\,(XI_m - AB)\text{dét}\,(XI_n) \\ &= X^n \chi_{AB}(X) \ . \end{aligned}$$

D'un autre côté,

$$NM = \left(\begin{array}{c|c} XI_m & 0 \\ \hline XB & XI_n - BA \end{array}\right)$$

donc

$$\begin{aligned} \text{dét}\,(NM) &= \text{dét}\,(XI_m)\text{dét}\,(XI_n - BA) \\ &= X^m \chi_{BA}(X) \ . \end{aligned}$$

Or, dét $(MN) =$ dét $(NM) =$ dét $M$ dét $N$. *q.e.d.*

**Remarque :** — Si $A, A' \in \mathscr{M}_n(\mathbb{K})$ sont des matrices semblables *i.e.* si

$$^\exists P \in \mathrm{GL}_n(\mathbb{K}),\ A = PA'P^{-1}$$

alors :

$$\begin{aligned} \chi_A(X) &= \chi_{P(A'P^{-1})}(X) \\ &= \chi_{(A'P^{-1})P}(X) \\ &= \chi_{A'}(X) \end{aligned}$$

autrement dit deux matrices semblables ont le même polynôme caractéristique.

En conséquence, on peut définir le polynôme caractéristique d'un endomorphisme :

**Définition 38** *Supposons que $E$ est de dimension finie. Si $u$ est un endomorphisme de $E$, alors toutes les matrices de $u$ dans une base de $E$ sont semblables donc ont le même polynôme caractéistique. Ce polynôme caractéristique commun est le polynôme caractéristique de $u$, noté $\chi_u(X)$.*

Concrétement, si $(e) = e_1, ..., e_n$ est une base de $E$, si $u$ est un endomorphisme de $E$, alors :

$$\chi_u(X) = \chi_A(X)$$

où $A := \text{Mat}(u)_{(e)}$.

## Spectre et racines du polynôme caractéristique

On peut réécrire la proposition 4.3.1 :

**Théorème 4.3.3** *Soit $A \in \mathscr{M}_n(\mathbb{K})$. Alors :*

$$\text{Sp}(A) = \{ \text{ valeurs propres de } A \} = \{ \text{ racines de } \chi_A(X) \}$$

*Démonstration* : On a $\lambda$ valeur propre de $A \Leftrightarrow$ dét$(A - \lambda I_n) = 0$ $\Leftrightarrow \chi_A(\lambda) = 0$. *q.e.d.*

En particulier :

**Corollaire 4.3.3.1** *Si $A \in \mathscr{M}_n(\mathbb{K})$, $A$ possède au plus $n$ valeurs propres.*

(En effet, nous savons qu'un polynôme de degré $n$ a au plus $n$ racines).

Exemple : [s]

— Si $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, alors

$$\chi_A(X) = X^2 - X - 1 = (X - \frac{1-\sqrt{5}}{2})(X - \frac{1+\sqrt{5}}{2})$$

donc $\text{Sp}_{\mathbb{R}}(A) = \{\frac{1-\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2}\}$ mais $\text{Sp}_{\mathbb{Q}}(A) = \emptyset$.

— Si $A = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, alors :

$$\chi_A(X) = X^2 + X + 1 = (X - j)(X - j^2)$$

où $j := -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Donc dans ce cas :

$$\text{Sp}_{\mathbb{C}}(A) = \left\{j, j^2\right\}$$

mais $\text{Sp}_{\mathbb{R}}(A) = \emptyset$.

— Si $A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, alors :

$$\chi_A(X) = X^2 - 2\cos\theta X + 1 = (X - e^{i\theta})(X - e^{-i\theta})$$

et $\mathrm{Sp}_{\mathbb{C}}(A) = \{e^{-i\theta}, e^{i\theta}\}$. (Si $\theta \neq 0 \bmod \pi$, alors $\mathrm{Sp}_{\mathbb{R}}(A) = \emptyset$).

**Cas des matrices triangulaires :**

Soit

$$T := \begin{pmatrix} t_{1,1} & \cdots & t_{1,n} \\ 0 & \ddots & \vdots \\ 0 & 0 & t_{n,n} \end{pmatrix}$$

une matrice triangulaire supérieure. Alors :

$$\chi_T(X) = \begin{vmatrix} X - t_{1,1} & \cdots & -t_{1,n} \\ 0 & \ddots & \vdots \\ 0 & 0 & X - t_{n,n} \end{vmatrix} = \prod_{i=1}^{n} (X - t_{i,i})$$

donc $\mathrm{Sp}_{\mathbb{K}}(T) = \{t_{i,i} \ : \ 1 \leq i \leq n\}$.

## Matrices compagnons :

Soit $P(X) := X^n + c_{n-1}X^{n-1} + ... + c_0 \in \mathbb{K}[X]$. On pose :

$$C_P := \begin{pmatrix} 0 & \cdots & 0 & -c_0 \\ 1 & \ddots & \vdots & \vdots \\ 0 & \ddots & 0 & \vdots \\ 0 & \cdots 0 & 1 & -c_{n-1} \end{pmatrix} \in \mathscr{M}_n(\mathbb{K})$$

c'est la *matrice compagnon* du polynôme $P$.

**Proposition 4.3.4**

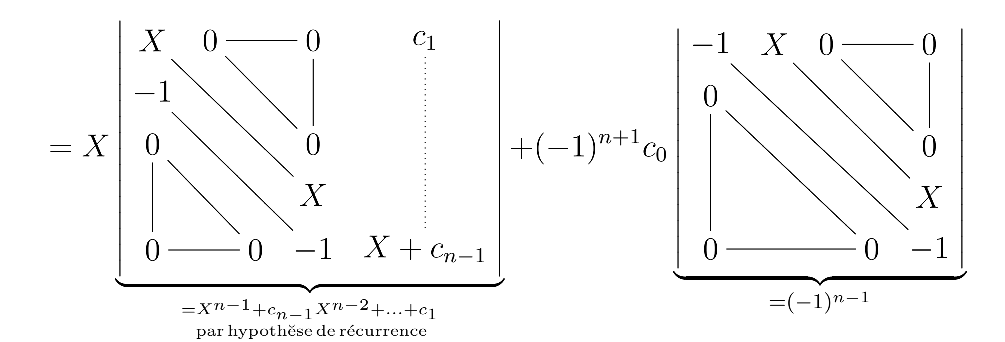
$$\chi_{C_P}(X) = P(X) \ .$$

*Démonstration :* Par récurrence sur $n \geq 1$. Si $n = 1$ c'est évident car $P(X) = X + c_0$ et $C_P = (-c_0)$ (matrice $1 \times 1$).

Si $P(X) = X^n + c_{n-1}X^{n-1} + ... + c_0$, on a :

$$\chi_{C_P}(X) = \begin{vmatrix} X & 0 & \cdots & 0 & c_0 \\ -1 & \ddots & \ddots & \vdots & \vdots \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & X & \vdots \\ 0 & \cdots & 0 & -1 & X + c_{n-1} \end{vmatrix}$$

(en développant par rapport à la première ligne)




$$= X^n + c_{n-1}X^{n-1} + ... + c_0$$
$$= P(X)$$

(ce qui achève la récurrence).

*q.e.d.*

Exemple : Soit $J$ la matrice :

$$\begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & \ddots & & 0 \\ 0 & \ddots & \ddots & \vdots \\ 0 & 0 & 1 & 0 \end{pmatrix} \in \mathscr{M}_n(\mathbb{K})$$

alors $\chi_J(X) = X^n - 1$ car $J = C_{X^n-1}$.

**Exercice 33 (Polynômes de Tchébychev)** *On rappelle le résultat suivant :*

*Pour tout $k$ entier $\geq 1$, il existe un polynôme en $t$, à coefficients rationnels, noté $T_k(t)$, tel que :*

$$\forall \theta \in \mathbb{R}, \sin(k\theta) = \sin\theta\, T_k(\cos\theta)$$

*(en effet :*

$$\begin{aligned} \sin(k\theta) &= \operatorname{Im}\,(e^{ik\theta}) \\ &= \operatorname{Im}\,\left((\cos\theta + i\sin\theta)^k\right) \end{aligned}$$

*et on développe ...)*

*Par exemple,* $\sin(2\theta) = \sin\theta(2\cos\theta)$ *et* $\sin(3\theta) = \sin\theta(4\cos^2\theta - 1)$ *donc* $T_2(t) = 2t$ *et* $T_3(t) = 4t^2 - 1$*. Plus généralement,* $T_k(t) = 2^{k-1}t^{k-1} + ...$

*Pour tout $n$ soit :*

$$V_n := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \in \mathscr{M}_n(\mathbb{R})$$

*alors, pour tout $n \geq 1$ :*

$$\chi_{V_n}(X) = T_{n+1}(\frac{X}{2})$$

*en particulier,*

$$\operatorname{Sp}_{\mathbb{R}}(V_n) = \left\{ 2\cos\left(\frac{k\pi}{n+1}\right) : \ 1 \leq k \leq n \right\} \ .$$

*Indications : vérifier que* $\chi_{V_n}(X) = T_{n+1}(\frac{X}{2})$ *pour* $n = 1, 2$ *et trouver une relation de récurrence d'ordre 2 pour* $\chi_{V_n}(X)$ *(en développant par rapport à une ligne ou une colonne) et une autre pour* $T_n(X)$*.*

Rappelons le

**Théorème 4.3.5 (fondamental de l'algèbre (ou théorème de d'Alembert))** *Tout polynôme complexe non constant admet une racine dans* $\mathbb{C}$*.*

*admettons ...*

**Corollaire 4.3.5.1** *Toute matrice* $A \in \mathscr{M}_n(\mathbb{C})$*,* $n \geq 1$*, tout endomorphisme $u$ d'un espace vectoriel* **complexe** *de* **dimension finie** *admet au moins une valeur propre.*

*Démonstration :* Le polynôme caractéristique de $A$ (ou de $u$) est un polynôme complexe non constant donc admet (au moins) une racine $\lambda \in \mathbb{C}$. Alors, $\lambda$ est une valeur propre de $A$ (ou de $u$). *q.e.d.*

**Corollaire 4.3.5.2** *Soit $A$ une matrice réelle. Alors, $A$ possède un sous-espace invariant de dimension 1 ou 2.*

*Démonstration :* Soit $n \geq 1$. Comme $A \in \mathscr{M}_n(\mathbb{R}) \subseteq \mathscr{M}_n(\mathbb{C})$, $A$ possède une valeur propre $\lambda = a + ib \in \mathbb{C}$, $a, b$ réels, et un vecteur propre associé $Z = X + iY \in \mathbb{C}^n \setminus \{0\}$ où $X, Y \in \mathbb{R}^n$.

Alors :

$$AZ = \lambda Z \Leftrightarrow AX + iAY = (aX - bY) + i(bX + aY)$$

$$\Leftrightarrow AX = aX - bY \text{ et } AY = bX + aY$$

et en particulier le sous-espace (réel) $\langle X, Y \rangle$ est stable par $A$. Or $X$ ou $Y \neq 0$ donc $\langle X, Y \rangle$ est de dimension 1 ou 2. *q.e.d.*

## 4.4 Espaces propres

**Définition 39** *Soit $A \in \mathscr{M}_n(\mathbb{K})$ (ou soit $u$ un endomorphisme de $E$). Soit $\lambda \in \mathbb{K}$ une valeur propre de $A$ (ou de $u$). L'espace propre de $A$ associé à la valeur propre $\lambda$ est le sous-espace vectoriel :*

$$E_\lambda(A) := \ker(A - \lambda I_n) = \{X \in \mathbb{K}^n \ : \ AX = \lambda X\}$$

*(version pour l'endomorphisme $u$ :*

$$E_\lambda(u) := \ker(u - \lambda I_n) = \{x \in E \ : \ u(x) = \lambda x\} \ )$$

**Remarque :** [s] — Si $\lambda$ est une valeur propre de $A$, l'espace propre associé $E_\lambda(A)$ est de dimension $\geq 1$ ;

— L'espace propre $E_\lambda(A)$ est invariant par $A$. En effet :

$$X \in \ker(A - \lambda I_n) \Rightarrow A(AX) = A(\lambda X) = \lambda(AX)$$

$$\Rightarrow AX \in \ker(A - \lambda I_n) \ .$$

**Théorème 4.4.1** *Soit $u$ un endomorphisme de $E$. Soient $\lambda_1, ..., \lambda_r$ $r$ valeurs propres* **distinctes** *de $u$. Alors les espaces propres associés $E_{\lambda_1}, ..., E_{\lambda_r}$ sont en somme directe* i.e. *:*

$$E_{\lambda_1} + .... + E_{\lambda_r} = E_{\lambda_1} \oplus .... \oplus E_{\lambda_r} \ .$$

**Remarque :** On en déduit que le nombre de valeurs propres est $\leq \dim E$ car :

$$\dim E \geq \dim E_{\lambda_1} \oplus .... \oplus E_{\lambda_r} = \dim E_{\lambda_1} + ... + \dim E_{\lambda_r} \geq r \ .$$

## Rappels sur les sommes directes

**Définition 40** *On dit que $E_1, ..., E_r$ des sous-espaces de $E$ sont en somme directe si :*

$$^\forall v_1 \in E_1, ..., ^\forall v_r \in E_r, \ v_1 + ... + v_r = 0 \Rightarrow v_1 = ... = v_r = 0$$

*notation :*

$$E_1 + ... + E_r = E_1 \oplus ... \oplus E_r \ .$$

**Remarque :** Si $r = 2$, $E_1$ et $E_2$ sont en somme directe si et seulement si $E_1 \cap E_2 = \{0\}$.

**Exercice 34** *$E_1, ..., E_r$ sont en somme directe $\Leftrightarrow$ :*

$$^\forall 1 \leq i \leq r, \ E_i \cap (\sum_{\substack{j=1 \\ j \neq i}}^{r} E_j) = \{0\} \ .$$

EXEMPLE : Si $e_1, ..., e_n$ est une famille libre de $E$ (par exemple une base), alors les droites $\mathbb{K}e_1, ..., \mathbb{K}e_n$ sont en somme directe.

Il est facile de calculer la dimension d'une somme directe :

**Proposition 4.4.2** *Si $E_1, ..., E_r$ sont des sous-espaces de $E$ en somme directe, alors :*

$$\dim(E_1 + ... + E_r) = \dim E_1 + ... + \dim E_r \ .$$

*Démonstration :* Soient $\mathscr{B}_1, ..., \mathscr{B}_r$ des bases respectives de $E_1, ..., E_r$. Alors les $\mathscr{B}_i$ sont deux à deux disjointes et $\mathscr{B}_1 \cup ... \cup \mathscr{B}_r$ est une base de $E_1 + ... + E_r$ donc :

$$\dim E_1 \oplus ... \oplus E_r = \left| \mathscr{B}_1 \cup ... \cup \mathscr{B}_r \right|$$

$$= \left| \mathscr{B}_1 \right| + ... + \left| \mathscr{B}_r \right|$$

$$\dim E_1 + ... + \dim E_r \ .$$

*q.e.d.*

*

*Démonstration du théorème :* Par récurrence sur $r \geq 1$. Si $r = 1$, il n'y a rien à démontrer.

Soient $v_1 \in E_{\lambda_1}, ..., v_r \in E_{\lambda_r}$ tels que

$$v_1 + ... + v_r = 0 \qquad (4.1)$$

alors si on applique $u$, on trouve :

$$u(v_1) + ... + u(v_r) = 0 \qquad (4.2)$$

$$\Leftrightarrow \lambda_1 v_1 + ... + \lambda_r v_r = 0 \qquad (4.3)$$

mais alors (4.1) - $\lambda_1$ x (4.3) donne :

$$(\lambda_2 - \lambda_1)v_2 + ... + (\lambda_r - \lambda_1)v_r = 0$$

$\Rightarrow$(hypothèse de récurrence de rang $r-1$)$\Rightarrow$ :

$$(\lambda_2 - \lambda_1)v_2 = ... = (\lambda_r - \lambda_1)v_r = 0$$

$$\Rightarrow v_2 = ... = v_r = 0$$

car $\lambda_2 - \lambda_1, ..., \lambda_r - \lambda_1 \neq 0$.

On a donc aussi : $v_1 = -v_2 - ... - v_r = 0$. *q.e.d.*

**Corollaire 4.4.2.1** *Soit $A \in \mathscr{M}_n(\mathbb{K})$. Si le polynôme caractéristique de $A$ possède $n$ racines distinctes dans $\mathbb{K}$, alors il existe une base de $\mathbb{K}^n$ formée de vecteurs propres de $A$.*

*Démonstration :* Soient $\lambda_1, ..., \lambda_n \in \mathbb{K}$ les $n-$racines distinctes de $\chi_A(X)$. Ce sont aussi $n$ valeurs propres de $A$. Notons $E_{\lambda_1}$,...,$E_{\lambda_n}$ les espaces propres associés. Alors : $E_{\lambda_1} + ... + E_{\lambda_n} \subseteq E$ et :

$$\dim(E_{\lambda_1} + ... + E_{\lambda_n}) = \dim(E_{\lambda_1} \oplus ... \oplus E_{\lambda_n})$$

$$= \dim E_{\lambda_1} + ... + \dim E_{\lambda_n} \geq n = \dim \mathbb{K}^n$$

donc :

$$^\forall 1 \leq i \leq n, \dim E_{\lambda_i} = 1 \text{ et } E_{\lambda_1} \oplus ... \oplus E_{\lambda_n} = \mathbb{K}^n \ .$$

Pour tout $i$, soit $e_i$ un vecteur non nul tel que :

$$E_{\lambda_i} = \mathbb{K}e_i$$

alors les vecteurs $e_i$ sont des vecteurs propres de $A$ (de valeurs propres $\lambda_i$) et

$$\mathbb{K}e_1 + ... + \mathbb{K}e_n = \mathbb{K}e_1 \oplus ... \oplus \mathbb{K}e_n = \mathbb{K}^n$$

signifie que les $e_i$ forment une base de $\mathbb{K}^n$. *q.e.d.*

**Remarque :** Bien entendu la réciproque est fausse car par exemple si $n \geq 2$, il existe toujours une base formée de vecteurs propres de $I_n$ mais son polynôme caractéristique, $\chi_{I_n}(X) = (X-1)^n$ n'a qu'une seule racine : 1.

**Définition 41 (diagonalisable)** *On dit qu'une matrice $A$ (resp. un endomorphisme $u$ de $E$) est diagonalisable s'il existe une base de $\mathbb{K}^n$ (respectivement de $E$) formée de vecteurs propres de $A$ (respectivement de $u$).*

**Remarque :** Si $u$ est diagonalisable et si on note $\lambda_1, ..., \lambda_r$ ses valeurs propres distinctes, alors :

$$\ker(u - \lambda_1 \mathrm{Id}_E) \oplus .... \oplus \ker(u - \lambda_r \mathrm{Id}_E) = E$$

(car tout vecteur de $E$ est combinaison linéaire de vecteurs propres de $u$ donc est une somme de vecteurs appartenant aux espaces propres $\ker(u - \lambda_i)$) et réciproquement, si :

$$\ker(u - \lambda_1 \mathrm{Id}_E) \oplus .... \oplus \ker(u - \lambda_r \mathrm{Id}_E) = E$$

alors, il existe une base de $E$ formée de vecteurs propres de $u$ (il suffit de mettre « bout à bout » des bases des espaces propres $\ker(u - \lambda_i \mathrm{Id}_E)$).

En bref :

$$u \text{ est diagonalisable } \Leftrightarrow \ker(u - \lambda_1 \mathrm{Id}_E) \oplus .... \oplus \ker(u - \lambda_r \mathrm{Id}_E) = E \ .$$

Si $A$ est une matrice diagonalisable et si $P$ est une matrice de passage de la base canonique de $\mathbb{K}^n$ dans une base de vecteurs propres, $v_1, ..., v_n$ alors

$$A = PDP^{-1}$$

où $D$ est une matrice diagonale : si $\lambda_1, ..., \lambda_n$ sont les valeurs propres correspondant respectivement aux vecteurs $v_1, ..., v_n$, alors :

$$D = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \ .$$

*Diagonaliser* une matrice $A \in \mathscr{M}_n(\mathbb{K})$ signifie trouver, si elles existent, $P \in \mathrm{GL}_n(\mathbb{K})$, $D \in \mathscr{M}_n(\mathbb{K})$ diagonale telles que :

$$A = PDP^{-1} \ .$$

Exemple : — Toute matrice réelle $2 \times 2$ symétrique :

$$\begin{pmatrix} a & b \\ b & d \end{pmatrix}$$

est diagonalisable (*exo*)

— **projections :** On suppose que $E = F \oplus G$. On définit la projection sur $F$ suivant $G$ par :

$$p : E \to E \, , \underbrace{x}_{\in F} \oplus \underbrace{y}_{\in G} \mapsto x \ .$$

Il est facile de voir que :

$$F = \ker(p - \mathrm{Id}_E) = E_1(p) \text{ et } G = \ker p = E_0(p)$$

donc $p$ est diagonalisable. Remarquer aussi que $p^2 = p$. En fait, réciproquement, si $p$ est un endomorphisme de $E$ tel que $p^2 = p$ alors $p$ est une projection sur un certain sous-espace suivant un autre certain sous-espace.

— **réflexions :** On suppose encore que $E = F \oplus G$. On définit la réflexion par rapport à $F$ suivant $G$ par :

$$r : E \to E \, , \underbrace{x}_{\in F} \oplus \underbrace{y}_{\in G} \mapsto x - y$$

c'est un endomorphisme de $E$ tel que : $r^2 = \mathrm{Id}_E$. Il est facile de voir :

$$F = \ker(r - \mathrm{Id}_E) = E_1(r) \text{ et } G = \ker(r + \mathrm{Id}_E) = E_{-1}(r) \ .$$

Vérifier que si $r$ est un endomorphisme de $E$ vérifiant $r^2 = \mathrm{Id}_E$ ($\mathbb{K} = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$), alors $r$ est une réflexion par rapport à un certain sous-espace et suivant un certain autre sous-espace.

— La matrice de permutation circulaire

$$J = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & \ddots & & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \\ 0 & \cdots\ 0 & 1 & 0 \end{pmatrix} \in \mathscr{M}_n(\mathbb{K})$$

est diagonalisable sur $\mathbb{C}$ de valeurs propres

$$1, e^{i\frac{2\pi}{n}}, ..., e^{i\frac{2(n-1)\pi}{n}}$$

les racines $n-$ièmes de l'unité. Trouver une base de vecteurs propres (*exo*) .

## 4.5 Un premier critère de diagonalisabilité

### Rappels sur les polynômes

**Définition 42** *Un polynôme à coefficients dans* $\mathbb{K}$ *est une suite*

$$a_0, a_1, a_2, ...$$

*dont tous les termes sont nuls à partir d'un certain rang et qui est notée :*

$$a_0 + a_1 X + a_2 X^2 + ...$$

*Le degré du polynôme*

$$P(X) = a_0 + a_1 X + ...$$

*est le plus grand entier* $n$*, noté* $\deg P$*, tel que* $a_n \neq 0$*. On prend pour convention* $\deg 0 = -\infty$.

*Si* $P(X) = a_0 + a_1 X + ...$ *et* $Q(X) = b_0 + b_1 X + ...$ *sont des polynômes, on définit leur produit :*

$$P(X)Q(X) := a_0 b_0 + (a_0 b_1 + a_1 b_0)X + ... + (a_0 b_k + a_1 b_{k-1} + ... + a_k b_0)X^k + ...$$

*On note* $\mathbb{K}[X]$ *la* $\mathbb{K}-$*algèbre des polynômes à coefficients dans* $\mathbb{K}$.

**Remarque :** [importante] On peut attribuer une valeur à $X$ : si $P(X) = a_0 + ... + a_d X^d$, si $\lambda \in \mathbb{K}$, on définit :

$$P(\lambda) := a_0 + ... + a_d \lambda^d \in \mathbb{K} \ .$$

**Remarque :** Pour tous polynômes $P(X)$, $Q(X)$ à coefficients dans $\mathbb{K}$, $\deg(PQ) = \deg P + \deg Q$.

**Proposition 4.5.1 (intégrité)** *Soient $P(X), Q(X) \in \mathbb{K}[X]$. Si $P(X)Q(X) = 0$, alors $P(X) = 0$ ou $Q(X) = 0$.*

*Démonstration :* Si $P(X) \neq 0$ et $Q(X) \neq 0$, alors, $\deg(PQ) = \deg P + \deg Q \geq 0$ donc $P(X)Q(X) \neq 0$. *q.e.d.*

### Divisibilité, racines, multiplicité

**Définition 43** *Si $P(X), Q(X) \in \mathbb{K}[X]$, on dit que $Q$ divise $P$ (dans $\mathbb{K}[X]$) si*

$$P(X) = B(X)Q(X)$$

*pour un certain polynôme $B(X) \in \mathbb{K}[X]$. Notation :*

$$Q|P$$

*remarque :*

$$Q|P \Rightarrow \deg Q \leq \deg P \ .$$

**Formule de Taylor :**

Pour tout $P(X) \in \mathbb{K}[X]$, pour tout $\lambda \in \mathbb{K}$, il existe (une unique) suite $a_0, ..., a_d$ telle que :

$$P(X) = a_0 + a_1(X - \lambda) + ... + a_d(X - \lambda)^d$$

Bien entendu, $a_0 = P(\lambda)$. On dit que $\lambda$ est une racine de $P$ si $P(\lambda) = 0$ *i.e.* si $(X - \lambda)|P(X)$.

Si $P(X) \neq 0$, on appelle *multiplicité* de $\lambda$ dans $P$ le plus petit entier $i$ tel que $a_i \neq 0$.

Autrement dit la multiplicité de $\lambda$ dans $P$ est le plus grand entier $i$ tel que $(X - \lambda)^i|P(X)$.

**Notation :** $\text{mult}_\lambda P :=$ la multiplicité de $\lambda$ dans $P$. **Remarque :** Soient $P \in \mathbb{K}[X]$, $\lambda \in \mathbb{K}$. On a l'équivalence :

$$\lambda \text{ racine de } P \ \Leftrightarrow \text{mult}_\lambda P \geq 1 \ .$$

**Exercice 35 Multiplicité du produit :**

$$\forall P, Q \in \mathbb{K}[X], \forall \lambda \in \mathbb{K},\ mult_\lambda(PQ) = mult_\lambda P + mult_\lambda Q$$

**Remarque :** [multiplicité] Si $\lambda_1, ..., \lambda_r$ sont deux à deux distincts et si :

$$P(X) := (X - \lambda_1)^{m_1} ... (X - \lambda_r)^{m_r}$$

alors $m_i$ est la multiplicité de $\lambda_i$ dans $P(X)$, pour tout $i$. En effet, par exemple pour $i = 1$, d'après l'exercice précédent,

$$\begin{aligned} \mathrm{mult}_{\lambda_1} P &= m_1 \underbrace{\mathrm{mult}_{\lambda_1}(X - \lambda_1)}_{=1} + ... + m_r \underbrace{\mathrm{mult}_{\lambda_1}(X - \lambda_r)}_{=0} \\ &= m_1 \ . \end{aligned}$$

**Exercice 36** *Si* $\mathbb{K} = \mathbb{C}$ *montrer que :*

$$\sum_{\lambda \in \mathbb{C}} mult_\lambda P = \deg P$$

*pour tout polynôme non nul* $P$*.*

**Définition 44 (scindé)** *Un polynôme* $P(X)$ *est scindé sur* $\mathbb{K}$ *si :*

$$P(X) = a_d(X - \lambda_1) ... (X - \lambda_d)$$

*pour certains* $\lambda_i \in \mathbb{K}$ *et un* $a_d \in \mathbb{K}$*. Souvent, on regroupe les racines égales et on écrit :*

$$P(X) = a_d(X - \lambda_1)^{m_1} ... (X - \lambda_r)^{m_r}$$

*avec les* $\lambda_i$ *deux à deux distinctes et des entiers* $m_i \geq 1$*.*

Exemple : D'après le théorème de d'Alembert, tous les polynômes sont scindés sur $\mathbb{C}$.

*

Pour énoncer un premier critère de diagonalisation des endomorphismes on aura besoin du lemme suivant :

**Lemme 4.5.2** *Soit* $u$ *un endomorphisme de* $E$*. On suppose* $E$ *de dimension finie et on suppose aussi qu'il existe un sous-espace* $F$ *de* $E$ *invariant par* $u$*. Notons* $\chi_{u|_F}$ *le polynôme caractéristique de la restriction à* $F$*. Alors :*

$$\chi_{u|_F}(X) | \chi_u(X)$$

*dans* $\mathbb{K}[X]$*.*

*Démonstration :* Soit $e_1, ..., e_k$ une base de $F$ que l'on complète en une base de $E$ :

$$e_1, ..., e_n$$

alors la matrice de $u$ dans la base $e_1, ..., e_n$ est de la forme :

$$\begin{pmatrix} \overbrace{A}^{k} & \overbrace{B}^{n-k} \\ 0 & D \end{pmatrix} \begin{matrix} \}k \\ \}n-k \end{matrix}$$

(où $A$ est la matrice de $u|_F$ dans la base $e_1, .., e_k$). Mais alors :

$$\chi_u(X) = \begin{vmatrix} XI_k - A & -B \\ 0 & XI_{n-k} - D \end{vmatrix} = \text{dét}\,(XI_k - A)\text{dét}\,(XI_{n-k} - D)$$

$$= \chi_{u|_F}\,\text{dét}\,(XI_{n-k} - D) \ .$$

*q.e.d.*

**Définition 45 (multiplicités algébrique et géométrique)** *Soit $A \in \mathscr{M}_n(\mathbb{K})$. Soit $\lambda \in \mathbb{K}$. On notera $m_a(\lambda)$ la multiplicité de $\lambda$ dans le polynôme caractéristique de $A$, $\chi_A(X)$ :*

$$m_a(\lambda) := \text{ le plus grand entier } m \text{ tel que } (X - \lambda)^m | \chi_A(X)$$

*c'est la multiplicité algébrique de $\lambda$. On notera :*

$$m_g(\lambda) := \dim_{\mathbb{K}} \ker(A - \lambda I_n)$$

*c'est la multiplicité géométrique de $\lambda$.*

**Corollaire 4.5.2.1** *Soit $A \in \mathscr{M}_n(\mathbb{K})$ ou soit $u$ un endomorphisme de $E$, si $E$ est de dimension finie. Pour tout $\lambda \in \mathbb{K}$,*

$$m_g(\lambda) \leq m_a(\lambda) \ .$$

Exemple : Si

$$A = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ & & & \ddots & 1 \\ 0 & \cdots & & 0 & 1 \end{pmatrix} \in \mathscr{M}_n(\mathbb{K})$$

alors $\chi_A(X) = (X-1)^n$ et $m_g(1) = 1 < m_a(1) = n$.

Si $A = I_n$, alors : $\chi_A(X) = (X-1)^n$ et $m_g(1) = m_a(1) = n$.

*Démonstration :* Soit $\lambda$ une valeur propre de $u$. Posons $F := \ker(u-\lambda)$ l'espace propre associé.

Alors $F$ est stable par $u$ :

en effet, si $x \in F$, alors :

$$u(u(x)) = u(\lambda x) = \lambda u(x)$$

donc $u(x) \in F$.

Donc d'après le lemme 4.5.2,

$$\chi_{u|_F}(X) \,\Big|\, \chi_u(X)$$

or :

$$^\forall x \in F\,, u(x) = \lambda x$$

donc $u|_F = \lambda \mathrm{Id}_F$ et

$$\begin{aligned}\chi_{u|_F}(X) &= (X-\lambda)^{\dim F}\\ &= (X-\lambda)^{m_g(\lambda)}\end{aligned}$$

et finalement,

$$(X-\lambda)^{m_g(\lambda)} \,\Big|\, \chi_u(X) \Rightarrow m_g(\lambda) \le m_a(\lambda)\ .$$

<u>*q.e.d.*</u>

Voici un premier critère de diagonalisabilité :

**Théorème 4.5.3** *Soit $A \in \mathscr{M}_n(K)$ (respectivement $u$ un endomorphisme de $E$ avec $E$ de dimension finie). Alors :*

$$A \text{ (respectivement } u\text{) est diagonalisable sur } \mathbb{K} \Leftrightarrow \begin{cases} i)\ \chi_A(X) \text{ est scindé sur } \mathbb{K}\,; \\ \text{et} \\ ii)^\forall\lambda, \text{ valeur propre de } A,\ m_a(\lambda) = m_g(\lambda)\ . \end{cases}$$

*Démonstration :* $\Rightarrow$ : Supposons $u$ diagonalisable. Soient $\lambda_1, ..., \lambda_r$ les valeurs propres distinctes de $u$. Comme :

$$\ker(u - \lambda_1 \mathrm{Id}_E) \oplus ... \oplus \ker(u - \lambda_r \mathrm{Id}_E) = E\,,$$

si on choisit des bases $\mathscr{B}_1$ de $\ker(u - \lambda_1 \mathrm{Id}_E)$, ..., $\mathscr{B}_r$ de $\ker(u - \lambda_r \mathrm{Id}_E)$, on obtient une base $\mathscr{B}_1 \cup ... \cup \mathscr{B}_r$ de $E$ dans laquelle la matrice de $u$ est :

$$\mathrm{Mat}(u) = \left(\begin{array}{c|c|c} \lambda_1 I_{n_1} & & \\ \hline & \ddots & \\ \hline & & \lambda_r I_{n_r} \end{array}\right)$$

où $n_i = m_g(\lambda_i) = \dim \ker(u - \lambda_i \mathrm{Id}_E)$ pour tout $i$. Donc :

$$\chi_u(X) = (X - \lambda_1)^{n_1} ... (X - \lambda_r)^{n_r} \ .$$

Par conséquent le polynôme $\chi_u(X)$ est scindé sur $\mathbb{K}$ et :

$$^\forall i,\ m_a(\lambda_i) = n_i = m_g(\lambda_i) \ .$$

$\Leftarrow$ : Supposons que :

$$\chi_u(X) = (X - \lambda_1)^{n_1} ... (X - \lambda_r)^{n_r}$$

pour certains $\lambda_i \in \mathbb{K}$, deux à deux distincts et certains entiers $n_i \geq 1$. Comme :

$$\ker(u - \lambda_1 \mathrm{Id}_E) + ... + \ker(u - \lambda_r \mathrm{Id}_E) = \ker(u - \lambda_1 \mathrm{Id}_E) \oplus ... \oplus \ker(u - \lambda_r \mathrm{Id}_E) \subseteq E\,,$$

on a :

$$\begin{aligned} m_g(\lambda_1) + ... + m_g(\lambda_r) &= \dim\left(\ker(u - \lambda_1 \mathrm{Id}_E) + ... + \ker(u - \lambda_r \mathrm{Id}_E)\right) \\ &\leq \dim E \ . \end{aligned}$$

Or, pour tout $i$, $m_g(\lambda_i) = m_a(\lambda_i) = n_i$ et

$$n_1 + ... + n_r = \deg \chi_u = \dim E$$

en conséquence :

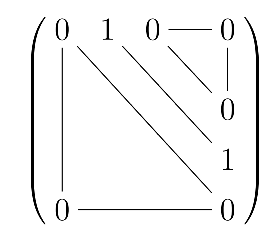
$$\dim\left(\ker(u - \lambda_1 \mathrm{Id}_E) + ... + \ker(u - \lambda_r \mathrm{Id}_E)\right) = \dim E$$

et forcément,

$$\ker(u - \lambda_1 \mathrm{Id}_E) + ... + \ker(u - \lambda_r \mathrm{Id}_E) = E \ .$$

*q.e.d.*

EXEMPLE : Si $n \geq 2$, la matrice :



n'est jamais diagonalisable car $m_g(0) = 1 < m_a(0) = n$.

## Méthode pour diagonaliser

Soit $A$ une matrice carrée complexe $n \times n$. Pour la diagonaliser :
— on calcule d'abord son polynôme caractéristique $\chi_A(X)$ ;
— on cherche les racines de $\chi_A(X)$ : ce sont les valeurs propres de $A$ ;
— pour toute valeur propre $\lambda$ de $A$, on cherche une base de $\ker A - \lambda I_n$ *i.e.* on cherche une base de l'espace des solutions du système :

$$AX = \lambda X$$

— si pour toute valeur propre $\lambda$ de $A$, $\dim \ker(A - \lambda I_n) = m_a(\lambda)$, $A$ est diagonalisable et une réunion des bases des espaces propres forme une base de vecteurs propres.

# 4.6 Trigonalisation

**Définition 46** *On dit qu'une matrice $A \in \mathscr{M}_n(K)$ (respectivement un endomorphisme $u$ de $E$, si $E$ est de dimension finie) est trigonalisable sur* $\mathbb{K}$ *(on devrait dire triangularisable mais ce terme signifie déjà autre chose) si $A$ est semblable à une matrice triangulaire supérieure c-à-d :*

$$^{\exists}P \in \mathrm{GL}_n(\mathbb{K}),\ T \in \mathscr{M}_n(\mathbb{K}),\ ^{\forall}n \geq i > j \geq 1,\ T_{i,j} = 0 \text{ et } A = PTP^{-1}$$

*(respectivement il existe une base de $E$ où la matrice de $u$ est triangulaire supérieure).*

**Exercice 37** *Toute matrice triangulaire inférieure est trigonalisable (si $T$ est triangulaire inférieure, $w_0 T w_0^{-1}$ est triangulaire supérieure où :*

$$w_0 := \begin{pmatrix} 0 & \cdots & 0 & 1 \\ \vdots & & & 0 \\ 0 & & & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix} .$$

**Théorème 4.6.1** *Soit $A \in \mathscr{M}_n(\mathbb{K})$. Alors $A$ est trigonalisable $\Leftrightarrow \chi_A(X)$ est scindé sur $\mathbb{K}$.*

*Démonstration* : $\Rightarrow$ : Deux matrices semblables ont le même polynôme caractéristique donc il suffit de montrer que $\chi_T(X)$ est scindé pour toute matrice triangulaire supérieure $T$ ; ce qui est facile.

$\Leftarrow$ : On raisonne aves $u$ un endomorphisme de $E$ (et on suppose $E$ de dimension finie). Par récurrence sur $\dim E$. Si $\dim E = 1$, il n'y a rien à démontrer. Si $\dim E > 1$, alors comme $\chi_u(X)$ est scindé,

$$\chi_u(X) = (X - \lambda_1)...(X - \lambda_n)$$

où $n = \dim E$ et où les $\lambda_i \in \mathbb{K}$ ne sont pas forcément distincts. Soit $e_1$ un vecteur propre associé à la valeur propre $\lambda_1$. On complète $e_1$ en une base : $e_1, ..., e_n$. Dans cette base, la matrice de $u$ est de la forme :

$$\left(\begin{array}{c|c} \lambda_1 & l \\ \hline 0 & B \end{array}\right)$$

où $B \in \mathscr{M}_{n-1}(\mathbb{K})$ et $l \in \mathscr{M}_{1,n-1}(\mathbb{K})$. En particulier,

$$\chi_u(X) = (X - \lambda_1)\chi_B(X)$$

$$\Rightarrow \chi_B(X) = (X - \lambda_2)...(X - \lambda_n)$$

est scindé sur $\mathbb{K}$. Par hypothèse de récurrence, il existe $S \in \mathscr{M}_{n-1}(\mathbb{K})$ une matrice triangulaire supérieure et $Q \in \mathrm{GL}_{n-1}(\mathbb{K})$ une matrice inversible telles que :

$$B = QSQ^{-1}$$

alors, on peut vérifier que :

$$\mathrm{Mat}(u) = \left(\begin{array}{c|c} \lambda_1 & l \\ \hline 0 & QSQ^{-1} \end{array}\right)$$

$$= P \left(\begin{array}{c|c} \lambda_1 & lQ \\ \hline 0 & S \end{array}\right) P^{-1}$$

pour la matrice inversible :

$$P := \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & Q \end{array}\right) .$$

Donc la matrice de $u$ dans la base $e_1, ..., e_n$ est semblable à une matrice triangulaire supérieure :

$$\left(\begin{array}{c|c} \lambda_1 & lQ \\ \hline 0 & S \end{array}\right)$$

donc $u$ est trigonalisable. *q.e.d.*

**Corollaire 4.6.1.1** *Sur $\mathbb{C}$ toutes les matrices sont trigonalisables.*

## Relations entre les valeurs propres et les invariants

Soit $A \in \mathscr{M}_n(\mathbb{C})$. Alors $A$ est semblable à une matrice triangulaire supérieure de la forme :

$$\begin{pmatrix} \lambda_1 & \cdots & \cdots \\ 0 & \ddots & \vdots \\ 0 & 0 & \lambda_n \end{pmatrix} \tag{4.4}$$

donc :

$$\chi_A(X) = (X - \lambda_1)...(X - \lambda_n)$$

ainsi les coefficients diagonaux de (4.4) ne dépendent que de $A$ :

ce sont les valeurs propres de $A$ comptées avec leur multiplicité algébrique.

**Exercice 38** *Vérifier que*

$$\text{dét}\, A = \lambda_1 ... \lambda_n$$

$$\forall k \geq 1,\ \text{tr} A^k = \lambda_1^k + ... + \lambda_n^k\ .$$

On peut en déduire la belle formule suivante :

$$\exists \epsilon > 0,\ \forall |t| < \epsilon\,,$$

la série $\displaystyle\sum_{k=1}^{\infty} \frac{\text{tr}(A^k)}{k} t^k$ converge, la matrice $I_n - tA$ est inversible et :

$$e^{\left(\sum_{k=1}^{\infty} \frac{\text{tr} A^k}{k} t^k\right)} = \frac{1}{\text{dét}\,(I_n - tA)}\ .$$

# Chapitre 5

# Polynômes d'endomorphismes

Soit $u$ un endomorphisme d'un espace vectoriel $E$ sur $\mathbb{K}$. Soit $A \in \mathscr{M}_n(\mathbb{K})$.

## 5.1 Définition

On remplace $X^k$ par $u^k$ (ou $A^k$) et 1 par $\mathrm{Id}_E$ (ou $I_n$).
Soit $P(X) = a_0 + a_1X + a_2X^2 + ... \in \mathbb{K}[X]$ un polynôme. On pose :

$$P(u) := a_0\mathrm{Id}_E + a_1u + a_2u^2 + ... \text{ et } P(A) := a_0I_n + a_1A + a_2A^2 + ...$$

**Proposition 5.1.1** *L'application :*

$$\mathbb{K}[X] \to \mathscr{M}_n(\mathbb{K})\,,\; P(X) \mapsto P(A)$$

*est un morphisme d'algèbres* i.e. *: c'est linéaire et :*

$$^\forall P, Q \in \mathbb{K}[X]\,,\; (PQ)(A) = P(A)Q(A)$$

*de même l'application :*

$$\mathbb{K}[X] \to \mathrm{End}_{\mathbb{K}}(E)\,,\; P(X) \mapsto P(u)$$

*est aussi un morphisme d'algèbres.*

*Démonstration :* Si $P(X) = a_0 + a_1X + ...$ et $Q(X) = b_0 + b_1X + ...$, alors $PQ(X) = a_0b_0 + (a_0b_1 + a_1b_0)X + ....$ Donc :

$$(PQ)(A) = a_0b_0I_n + (a_0b_1 + a_1b_0)A + ...$$

$$= (a_0I_n + a_1A + ...)(b_0I_n + b_1A + ...)$$

$$= P(A)Q(A) \ .$$

*q.e.d.*

**Remarque :** [importante] En particulier, pour tous $P, Q \in \mathbb{K}[X]$, les matrices $P(A)$ et $Q(A)$ commutent :

$$P(A)Q(A) = Q(A)P(A)$$

de même les endomorphismes $P(u)$ et $Q(u)$ commutent.

Exemple : — **Polynôme d'une diagonale :**

$$D := \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$$

on a :

$$P(D) = \begin{pmatrix} P(\lambda_1) & & \\ & \ddots & \\ & & P(\lambda_n) \end{pmatrix}$$

pour tout polynôme $P(X) \in \mathbb{K}[X]$.

— **polynôme et conjugaison :** Si $Q$ est inversible, si $A = QA'Q^{-1}$, alors pour tout polynôme $P(X) \in \mathbb{K}[X]$, $P(A) = QP(A')Q^{-1}$.

**Exercice 39** *Montrer que plus généralement, pour une matrice triangulaire :*

$$T := \begin{pmatrix} \lambda_1 & \cdots & \vdots \\ & \ddots & \vdots \\ & & \lambda_n \end{pmatrix}$$

*on a :*

$$P(T) = \begin{pmatrix} P(\lambda_1) & \cdots & \vdots \\ & \ddots & \vdots \\ & & P(\lambda_n) \end{pmatrix}$$

*pour tout polynôme $P(X) \in \mathbb{K}[X]$ (les coefficients hors de la diagonale peuvent avoir une expression compliquée mais les coefficients diagonaux sont obtenus simplement en leur appliquant le polynôme $P$).*

## 5.2 Théorème de Cayley-Hamilton

**Définition 47** *On dit qu'un polynôme $P(X)$ est un polynôme annulateur de la matrice $A$ ou de l'endomorphisme $u$ si $P(A) = 0$, ou si $P(u) = 0$.*

EXEMPLE : — Si $p : E \to E$ est une projection, $X^2 - X$ est un polynôme annulateur de $p$ car $p^2 = p$.

— Si $r : E \to E$ est une réflexion, $X^2 - 1$ est un polynôme annulateur de $r$ car $r^2 = \mathrm{Id}_E$.

Où chercher les valeurs propres, connaissant un polynôme annulateur mais ne connaissant pas le polynôme caractéristique ?

**Proposition 5.2.1** *Si $P$ est un polynôme annulateur de $u$, respectivement de $A$, alors :*

$$\mathrm{Sp}(u) \subseteq \{ \textit{ racines de } P \ \}$$

*respectivement*

$$\mathrm{Sp}(A) \subseteq \{ \textit{ racines de } P \ \} \ .$$

*Démonstration :* Si $x$ est un vecteur propre de $u$ associé à une valeur propre $\lambda$, alors :

$$u(x) = \lambda x \Rightarrow {}^{\forall} k \geq 0 \, , u^k(x) = \lambda^k x$$

et plus généralement :

$$Q(u)(x) = Q(\lambda)x$$

pour tout polynôme $Q(X)$. En particulier : $P(u)(x) = 0 \Rightarrow P(\lambda)x = 0 \Rightarrow P(\lambda) = 0$ car $x \neq 0$. <u>*q.e.d.*</u>

**Théorème 5.2.2 (de Cayley-Hamilton)** *Si $E$ est de dimension finie,*

$$\chi_u(u) = 0$$

*de même $\chi_A(A) = 0$.*

EXEMPLE : — Si :

$$N := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ & & & & 0 \\ & & & \ddots & 1 \\ 0 & \cdots & & & 0 \end{pmatrix} \text{ et } J := \begin{pmatrix} 0 & \cdots & & 0 & 1 \\ 1 & \ddots & & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & & \ddots & \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \in \mathscr{M}_n(\mathbb{K}) \ ,$$

alors : $\chi_N(X) = X^n$ et $\chi_J(X) = X^n - 1$ et on a bien $N^n = 0$ et $J^n = I_n$.

*Démonstration (s) du théorème :*

**1ère démonstration (algébrique) :**

Notons $B(X) \in \mathscr{M}_n(\mathbb{K}[X])$ la transposée de la comatrice de $XI_n - A$. Tous les coefficients de la matrice $B(X)$ sont des polynômes à coefficients dans $\mathbb{K}$ de degré $\leq n-1$. Il existe donc des matrices :

$$B_0, ..., B_{n-1} \in \mathscr{M}_n(\mathbb{K})$$

telles que :

$$B(X) = B_0 + XB_1 + ... + X^{n-1}B_{n-1} \ .$$

On a alors :

$$B(X)(XI_n - A) = \text{dét}\,(XI_n - A)I_n$$

$$\Leftrightarrow (B_0 + XB_1 + ... + X^{n-1}B_{n-1})(XI_n - A) = \chi_A(X)I_n$$

(on développe la partie gauche)

$$\Leftrightarrow -B_0A + X(B_0 - B_1A) + X^2(B_1 - B_2A) + ... + X^{n-1}(B_{n-2} - B_{n-1}A) + X^nB_{n-1}$$

$$= \chi_A(X)I_n \qquad (5.1)$$

Notons $c_0, ..., c_n \in \mathbb{K}$ les coefficients du polynôme caractéristique :

$$\chi_A(X) = c_0 + ... + c_nX^n$$

($c_0 = \pm\text{dét}\,A, c_n = 1$) On a donc d'après (5.1) :

$$-B_0A = c_0I_n$$

$$B_0 - B_1A = c_1I_n$$

$$...$$

$$B_{n-1} = c_nI_n$$

et donc :

$$\chi_A(A) = c_0I_n + c_1A + ... + c_nA^n$$

$$= -B_0A + (B_0 - B_1A)A + (B_1 - B_2A)A^2 + ... + (B_{n-2}A^{n-1} - B_{n-1})A^{n-1} + B_{n-1}A^n$$

$$= 0$$

car « tout se simplifie » .

**2ème démonstration (avec les matrices compagnons) :** On suppose $E$ de dimension finie $n$. Soit $u$ un endomorphisme de $E$. Soit $v$ un vecteur non nul de $E$. Soit $1 \leq k \leq n$ le plus grand entier tel que la famille :

$$v, u(v), ..., u^{k-1}(v)$$

soit libre. Alors forcément, la famille

$$v, u(v), ..., u^{k-1}(v), u^k(v)$$

est liée et

$$u^k(v) + c_{k-1}u^{k-1}(v) + ... + c_0 v = 0$$

pour certains coefficients $c_0, ..., c_{k-1} \in \mathbb{K}$.

Posons : $F := \langle v, u(v), ..., u^{k-1}(v)\rangle$. C'est un sous-espace vectoriel de $E$ (de dimension $k$) stable par $u$. De plus la matrice de la restriction $u|_F$ dans la base

$$v, u(v), ..., u^{k-1}(v)$$

est la matrice :

$$A := \begin{pmatrix} 0 & \cdots & 0 & -c_0 \\ 1 & \ddots & \vdots & \vdots \\ 0 & \ddots & 0 & \vdots \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots 0 & 1 & -c_{n-1} \end{pmatrix}$$

C'est une matrice compagon donc :

$$\chi_A(X) = X^k + c_{k-1}X^{k-1} + ... + c_0 \ .$$

D'après le lemme 4.5.2, $\chi_A(X)$ divise $\chi_u(X)$ *c-à-d* :

$$\chi_u(X) = Q(X)\chi_A(X)$$

pour un certain polynôme $Q(X) \in \mathbb{K}[X]$. On a alors :

$$\chi_u(u)(v) = Q(u)\chi_A(u)(v)$$

$$= Q(u)(u^k(v) + c_{k-1}u^{k-1}(v) + ... + c_0 v)$$

$$= Q(u)(0) = 0$$

finalement $\chi_u(u)(v) = 0$ pour tout vecteur $v$ de $E$ et $\chi_u(u) = 0$.

**3ème démonstration (par les matrices triangulaires) :**

Supposons que $T$ est une matrice triangulaire :

$$T = \begin{pmatrix} t_1 & \cdots & \cdots \\ & \ddots & \vdots \\ & & t_n \end{pmatrix} .$$

Soient

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, ..., e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

les vecteurs de la base canonique de $\mathbb{K}^n$. On pose aussi :

$$V_k := \langle e_1, ..., e_k \rangle$$

si $1 \leq k \leq n$ et $V_0 := 0$. On a alors :

$$\forall 1 \leq k \leq n,\ (T - t_k I_n)(V_k) \subseteq V_{k-1}$$

donc :

$$\begin{aligned}(T - t_1 I_n)...(T - t_n I_n)(\mathbb{K}^n) &= (T - t_1 I_n)... \underbrace{(T - t_n I_n)(V_n)}_{\subseteq V_{n-1}} \\ &\subseteq (T - t_1 I_n)... \underbrace{(T - t_{n-1} I_n)(V_{n-1})}_{\subseteq V_{n-2}} \\ &\subseteq (T - t_1 I_n)... \underbrace{(T - t_{n-2} I_n)(V_{n-2})}_{\subseteq V_{n-3}} \\ &... \subseteq (T - t_1 I_n)(V_1) \subseteq V_0 = 0\end{aligned}$$

donc : $(T - t_1 I_n)...(T - t_n I_n) = 0$.

Or, $\chi_T(X) = (X - t_1)...(X - t_n)$. Donc :

$$\chi_T(T) = (T - t_1 I_n)...(T - t_n I_n) = 0 \ .$$

Soit $A \in \mathscr{M}_n(\mathbb{C})$. On sait que $A$ est trigonalisable *c-à-d* :

$$\exists P \in \mathrm{GL}_n(\mathbb{K}),\ \exists T \text{ triangulaire supérieure, } A = PTP^{-1} \ .$$

Mais alors $\chi_T(X) = \chi_A(X)$ et :

$$\chi_A(A) = P\chi_A(T)P^{-1} = P\chi_T(T)P^{-1} = 0 \ .$$

*q.e.d.*

## 5.3 Polynômes annulateurs

Un *polynôme annulateur* d'un endomorphisme $u$ de $E$ est un polynôme $P \in \mathbb{K}[X]$ tel que $P(u) = 0$. Par exemple, en dimension finie : $\chi_u(X)$. Un *polynôme minimal* de $u$ est un polynôme annulateur de $u$, non nul, de degré minimal.

EXEMPLE : Des polynômes minimaux des matrices :

$$O, I_n, N := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & & \cdots & 0 \end{pmatrix} \in \mathscr{M}_n(\mathbb{K}),$$

sont respectivement : $X, X-1, X^n$.

**Rappels sur la division euclidienne :**

Soient $P, Q$ deux polynômes dans $\mathbb{K}[X]$. Si $Q \neq 0$, alors il existe un unique couple $(B, R)$ tels que :

$$B, R \in \mathbb{K}[X],\ P = BQ + R \text{ et } \deg R < \deg Q$$

($R$ peut éventuellement être nul).

*Démonstration :* **Unicité :** si $B_0Q + R_0 = B_1Q + R_1 = P$ et $\deg R_{0,1} < \deg Q$ , alors $R_0 - R_1 = (B_0 - B_1)Q$ et $\deg(R_0 - R_1) < \deg Q$ ; donc forcément, $R_0 - R_1 = 0$ et $R_0 = R_1 \Rightarrow B_0 = B_1$.

**Existence :** On raisonne par récurrence sur le degré de $P$. Si $\deg P < \deg Q$, il suffit de choisir $B = 0$ et $R = P$. Sinon :

$$P = a_0 + \ldots + a_pX^p,\ Q = b_0 + \ldots + b_qX^q$$

avec $a_i, b_j \in \mathbb{K}$, $a_p, b_q \neq 0$, $p \geq q$.Il suffit alors d'appliquer l'hypothèse de récurrence au polynôme

$$P - \frac{a_p}{b_q}X^{p-q}Q$$

dont le degré est $< \deg P$. *q.e.d.*

*

**Proposition 5.3.1** *Soit $m_u(X)$ un polynôme minimal de $u$. Alors, $m_u$* DIVISE TOUS LES POLYNÔMES ANNULATEURS DE $u$.

*Démonstration :* Si $P(u) = 0$, on fait la division euclidienne de $P$ par $m_u$ :

$$P = Bm_u + R$$

où $\deg R < \deg m_u$. On a :

$$0 = P(u) = \underbrace{B(u)m_u(u)}_{=0} + R(u) \Rightarrow R(u) = 0$$

et $R(X)$ est un polynôme annulateur de $u$ de degré $< \deg m_u$. Forcément, $R = 0$ et $m_u(X) divise P(X)$. *q.e.d.*

Il existe donc au plus un *unique* polynôme minimal *unitaire* (*i.e.* son coefficient de plus haut degré vaut 1) de $u$ (*exo*) c'est LE polynôme minimal de $u$.

**Remarque :** Si $E$ est de dimension finie, $\chi_u(X)$ est un polynôme annulateur de $u$ (non nul) donc dans ce cas, le polynôme minimal existe toujours de plus :

$$m_u(X) \text{ divise } \chi_u(X)$$

dans $\mathbb{K}[X]$.

On définit de même les polynômes annulateurs et le polynôme minimal d'une matrice $A \in \mathscr{M}_n(\mathbb{K})$.

**Exercice 40** *Si $E$ est de dimension finie, le polynôme minimal de $u$ coïncide avec le polynôme minimal de sa matrice dans n'importe quelle base de $E$.*

**Proposition 5.3.2** *Soit $P$ un polynôme annulateur de $u$ un endomorphisme de $E$. Alors, pour tout $\lambda \in \mathrm{Sp}(u)$, $P(\lambda) = 0$. En particulier si le polynôme minimal $m_u$ existe, $m_u(\lambda) = 0$ pour toute valeur propre $\lambda$ de $u$.*

*Démonstration :* Si $u(x) = \lambda x$, $0 \neq x \in E$. Alors, $0 = P(u)(x) = P(\lambda)x \Rightarrow P(\lambda) = 0$. *q.e.d.*

**Proposition 5.3.3** *Les racines de $m_u(X)$ sont exactement les valeurs propres de $u$ c-à-d (si $m_u(X)$ existe) :*

$$\forall \lambda \in \mathbb{K}, \quad m_u(\lambda) = 0 \Leftrightarrow \lambda \in \mathrm{Sp}(u) \ .$$

*Démonstration :* Il suffit de démontrer que si $m_u(\lambda) = 0$, alors $\lambda$ est une valeur propre de $u$. Or dans ce cas, $m_u(X) = (X - \lambda)Q(X)$ pour un certain polynôme $Q(X)$ de degré $< \deg m_u(X)$. Donc :

$$0 = m_u(u) = (u - \lambda \mathrm{Id}_E)Q(u) \ .$$

Forcément $Q(u) \neq 0$ par minimalité de $m_u$. Donc $u - \lambda \mathrm{Id}_E$ n'est pas injective et donc $\lambda$ est une valeur propre de $u$. *q.e.d.*

**Comment trouver le polynôme minimal d'une matrice ?**

**Théorème 5.3.4** *Soit $A \in \mathscr{M}_n(\mathbb{K})$. On suppose que le polynôme caractéristique est scindé :*

$$\chi_A(X) = (X - \lambda_1)^{m_1} ... (X - \lambda_r)^{m_r}$$

*où $m_1, ..., m_r \geq 1$, $\lambda_1, ..., \lambda_r \in \mathbb{K}$, sont deux à deux distincts. Alors :*

$$m_A(X) = (X - \lambda_1)^{k_1} ... (X - \lambda_r)^{k_r}$$

*pour certains entiers : $1 \leq k_i \leq m_i$, $i = 1, ..., r$.*

*Démonstration :* On note $k_1, ..., k_r$ les multiplicités de $m_A(X)$ en les valeurs propres $\lambda_1, ..., \lambda_r$. On a déjà vu que $1 \leq k_i$ car $m_A(\lambda_i) = 0$. On a aussi $k_i \leq m_i$, la multiplicité de $\lambda_i$ dans $\chi_A(X)$. Il reste donc à démontrer le lemme suivant :

**Lemme 5.3.5** *On suppose que le polynôme $P(X)$ divise le produit*

$$(X - \lambda_1)^{m_1} ... (X - \lambda_r)^{m_r}$$

*dans $\mathbb{K}[X]$ pour certains $\lambda_i \in \mathbb{K}$ deux à deux distincts et certains entiers $m_i \geq 1$. Alors si on note $k_1, ..., k_r$ les multiplicités respectives des $\lambda_1, ..., \lambda_r$ dans $P(X)$, on a :*

$$P(X) = a_d (X - \lambda_1)^{k_1} ... (X - \lambda_r)^{k_r}$$

*où $a_d$ est le coefficient dominant de $P$.*

*Démonstration du lemme :* On peut supposer $P$ unitaire *i.e.* $a_d = 1$. On raisonne par récurrence sur $r \geq 0$. Si $r = 0$, il n'y a rien à montrer. Notons $Q(X) \in \mathbb{K}[X]$ le quotient par $P(X)$ :

$$(X - \lambda_1)^{m_1} ... (X - \lambda_r)^{m_r} = P(X) Q(X) \ .$$

La multiplicité de $\lambda_1$ dans $Q(X)$ est : $m_1 - k_1$. Donc :

$$P(X) = (X - \lambda_1)^{k_1} \widetilde{P}(X) \text{ et } Q(X) = (X - \lambda_1)^{m_1 - k_1} \widetilde{Q}(X)$$

d'où :

$$(X - \lambda_1)^{m_1} ... (X - \lambda_r)^{m_r} = (X - \lambda_1)^{m_1} \widetilde{P}(X) \widetilde{Q}(X)$$

$$\Leftrightarrow (X-\lambda_1)^{m_2}...(X-\lambda_r)^{m_r} = \widetilde{P}(X)\widetilde{Q}(X)$$

et on applique l'hypothèse de récurrence.

*q.e.d.*

**Remarque :** Un cas particulier important à retenir : les diviseurs unitaires de $(X-\lambda)^n$ sont les $(X-\lambda)^d$ avec $0 \le d \le n$ (pour tous $n \ge 0, \lambda \in \mathbb{K}$).

*q.e.d.*

**Exercice 41**

| | | | |
|---|---|---|---|
| $A$ | $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ |
| $\chi_A(X)$ | $X^4$ | $X^4$ | $X^4$ |
| $m_A(X)$ | $X^2$ | $X^3$ | $X^4$ |

**Exercice 42 (Polynôme minimal d'une diagonale)** *Soit*

$$D := \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$$

*alors* $m_D(X) = \prod_{\lambda \in \mathrm{Sp}(D)}(X-\lambda)$ *où* $\mathrm{Sp}(D) = \{\lambda_1, ..., \lambda_n\}$ *et les valeurs propres sont comptées sans multiplicité.*

**Nouveau critère de diagonalisabilité**

On dit qu'un polynôme $P(X) \in \mathbb{K}[X]$ est *scindé à racines simples dans* $\mathbb{K}$ s'il se factorise en :

$$P(X) = a_d(X-\lambda_1)...(X-\lambda_r)$$

où $0 \neq a_d \in \mathbb{K}$ et $\lambda_1, ..., \lambda_r \in \mathbb{K}$ sont deux à deux distincts.

**Théorème 5.3.6** *Une matrice* $A \in \mathscr{M}_n(\mathbb{K})$ *est diagonalisable sur* $\mathbb{K}$ *si et seulement si son polynôme minimal est scindé à racines simples sur* $\mathbb{K}$.

*Démonstration :* $\Rightarrow$ : Si $A$ est diagonalisable, $A$ est semblable à une diagonale. Or deux matrices semblables ont le même polynôme minimal (*exo*)

. Donc il suffit de calculer le polynôme minimal d'une matrice diagonale ce qui est l'objet d'un exercice précédent.

$\Leftarrow$ : Si $m_A(X) = (X - \lambda_1)...(X - \lambda_r)$ avec $\lambda_1, ..., \lambda_r \in \mathbb{K}$ deux à deux distincts, la décomposition en éléments simples de la fraction $\frac{1}{m_A(X)}$ donne :

$$\frac{1}{m_A(X)} = \frac{a_1}{X - \lambda_1} + ... + \frac{a_r}{X - \lambda_r}$$

où $a_i = \frac{1}{m'_A(\lambda_i)}$ pour tout $i$.

Donc

$$1 = a_1 Q_1(X) + ... + a_r Q_r(X)$$

où pur tout $i$ :

$$Q_i(X) = \frac{m_A(X)}{X - \lambda_i} = \prod_{\substack{j=1 \\ j \neq i}}^{r} (X - \lambda_j)$$

est un polynôme. Si on applique cette égalité à la matrice $A$, on trouve :

$$I_n = a_1 Q_1(A) + .. + a_r Q_r(A)$$

donc si $Z \in \mathbb{K}^n$, on a :

$$Z = a_1 Q_1(A)(Z) + .. + a_r Q_r(A)(Z)$$

or, pour tout $1 \leq i \leq r$, $Q_i(A)(Z) \in \ker(A - \lambda_i I_n)$ car :

$$(A - \lambda_i I_n)(Q_i(A)(Z)) = m_A(A)(Z) = 0 \ .$$

Par conséquent

$$\oplus_{i=1}^{r} \ker(A - \lambda_i I_n) = \mathbb{K}^n$$

et $A$ est diagonalisable.

*Remarque :* on peut utiliser aussi le lemme des noyaux. Si $m_A(X) = (X - \lambda_1)...(X - \lambda_r)$ avec $\lambda_1, ..., \lambda_r \in \mathbb{K}$ deux à deux distincts, on a :

$$m_A(A) = 0 \Leftrightarrow \mathbb{K}^n = \ker m_A(A) = \ker(A - \lambda_1 I_n) \oplus .... \oplus \ker(A - \lambda_r I_n)$$

car les polynômes $X - \lambda_i$ sont deux à deux premiers entre eux. En effet si $D(X)$ divise $X - \lambda_i$ et $X - \lambda_j$, $i \neq j$ dans $\mathbb{K}[X]$, alors $D(X)$ divise $X - \lambda_i - (X - \lambda_j) = \lambda_j - \lambda_i \in \mathbb{K} \setminus \{0\}$ donc $D(X)$ est constant. Donc $A$ est diagonalisable.

*q.e.d.*

**Lemme 5.3.7 (des noyaux)** *Soit $u$ un endomorphisme de $E$.*

*Soient $P(X), Q(X)$ des polynômes premiers entre eux. ALors :*

$$\ker((PQ)(u)) = \ker(P(u)) \oplus \ker(Q(u)) \ .$$

*Généralisation : soient $P_1, ..., P_r$ des polynômes deux à deux premiers entre eux. Alors :*

$$\ker(P_1...P_r)(u) = \ker(P_1(u)) \oplus ... \oplus \ker(P_r(u))$$

*(énoncés similaires avec des matrices)*

*Démonstration :*

**Rappels :** On dit que $P(X)$ et $Q(X)$ sont *premiers entre eux* si :

$$D(X) \in \mathbb{K}[X] \text{ divise } P(X) \text{ et } Q(X) \text{ dans } \mathbb{K}[X] \Rightarrow D(X)\text{constant} !$$

En particulier, sur $\mathbb{C}$, deux polynômes sont premiers entre eux si et seulement s'ils n'ont pas de racine commune.

**Proposition 5.3.8** *Soient $P, Q \in \mathbb{K}[X]$ alors :*

$$P, Q \text{ sont premiers entre eux } \Leftrightarrow \ ^{\exists}A, B \in \mathbb{K}[X],\ AP + BQ = 1 \ .$$

*Démonstration :* $\Leftarrow$ : (*exo*) $\Rightarrow$ : Soient $D \in \mathbb{K}[X]$ un polynôme non nul de degré minimal parmi les polynômes de la forme

$$AP + BQ\ ,\ A, B \in \mathbb{K}[X] \ .$$

Il suffit de montrer que $D$ est constant. On a donc $D = AP + BQ$. On fait la division euclidienne de $P$ par $D$ :

$$P = CD + R$$

pour un certain $C \in \mathbb{K}[X]$ et un certain $R \in \mathbb{K}[X]$ de degré $< \deg D$. Mais alors :

$$R = (1 - CA)P + (-CB)Q$$

donc par minimalité du degré de $D$, $R = 0$ et $D$ divise $P$. De même $D$ divise $Q$ donc $D$ est constant $= d \in K \setminus \{0\}$. D'où :

$$1 = \frac{A}{d}P + \frac{B}{d}Q \ .$$

*q.e.d.*

On écrit $1 = AP + BQ$ pour certains polynômes $A, B \in \mathbb{K}[X]$. On a donc :

$$\mathrm{Id}_E = P(u)A(u) + Q(u)B(u) \ .$$

Soit $x \in \ker((PQ)(u))$, alors :

$$x = P(u)A(u)(x) + Q(u)B(u)(x) \ .$$

Or,

$$P(u)Q(u)B(u)(x) = B(u)P(u)Q(u)(x) = 0 \ .$$

Donc $Q(u)B(u)(x) \in \ker(P(u))$. De même, $P(u)A(u)(x) \in \ker(Q(u))$. Donc :

$$x \in \ker(P(u)) + \ker(Q(u)) \ .$$

Réciproquement, il est clair que

$$\ker(P(u)) \subseteq \ker((PQ)(u)) \text{ et } \ker(Q(u)) \subseteq \ker((PQ)(u)) \ .$$

Donc :

$$\ker(PQ)(u) = \ker P(u) + \ker Q(u)$$

montrons que cette somme est directe : soit $x \in \ker P(u) \cap \ker Q(u)$. Alors :

$$x = A(u)P(u)(x) + B(u)Q(u)(x) = 0 \ .$$

Pour le cas général : on raisonne par récurrence sur $r$ :

Montrons d'abord que :

$$\ker(P_1(u)) + ... + \ker(P_r(u)) = \ker((P_1...P_r)(u)) \ .$$

Soit $x \in \ker((P_1...P_r)(u))$. Alors comme $P_1$ et $P_2$ sont premiers entre eux, on a :

$$1 = AP_1 + BP_2$$

pour certains polynômes $A, B \in \mathbb{K}[X]$. Donc en appliquant cette égalié à $u$ :

$$x = A(u)P_1(u)(x) + B(u)P_2(u)(x)$$

or : $A(u)P_1(u)(x) \in \ker(P_2...P_r)(u)$ car :

$$(P_2...P_r)(u)A(u)P_1(u)(x) = A(u)(P_1....P_r)(u)(x) = 0 \ .$$

Donc par hypothèse de récurrence :

$$A(u)P_1(u)(x) \in \ker(P_2(u)) + ... + \ker(P_r(u))$$

et de même :

$$B(u)P_2(u)(x) \in \ker(P_1(u)) + \ker(P_3(u)) + ... + \ker(P_r(u))$$

et donc :

$$x = A(u)P_1(u)(x) + B(u)P_2(u)(x) \in \ker(P_1(u)) + ... + \ker(P_r(u)) \ .$$

Il reste à montrer que cette somme est directe :
Supposons que

$$x_1 + ... + x_r = 0$$

pour certains $x_1 \in \ker(P_1(u)), ..., x_r \in \ker((P_r(u))$. si on applique $P_1(u)$, on trouve :

$$P_1(u)(x_2) + ... + P_1(u)(x_r) = 0$$

Or, $P_1(u)(x_2) \in \ker(P_2(u)), ..., P_1(u)(x_r) \in \ker((P_r(u))$ donc par hypothèse de récurrence :

$$P_1(u)(x_2) = ... = P_1(u)(x_r) = 0$$

Or : $\ker P_1(u) \cap \ker P_i(u) = 0$ si $i > 1$ car $P_1$ et $P_i$ sont premiers entre eux!.
Donc :

$$x_2 = ... = x_r = 0$$

et forcément, $x_1 = 0$. *q.e.d.*

**Corollaire 5.3.8.1** *Une matrice $A \in \mathscr{M}_n(\mathbb{K})$ est diagonalisable sur $\mathbb{K}$ si et seulement si elle admet un polynôme annulateur scindé à racines simples sur $\mathbb{K}$.*

**Corollaire 5.3.8.2** *Soit $u$ un endomorphisme de $E$ diagonalisable sur $\mathbb{K}$. Si $F$ est un sous-espace de $E$ stable par $u$, alors la restriction $u|_F$ est encore diagonalisable.*

*Démonstration :* En effet,

$$m_u(u) = 0 \Rightarrow m_u(u|_F) = 0 \Rightarrow m_{u|_F} \text{ divise } m_u$$

mais si $m_u$ est scindé à racines simples sur $\mathbb{K}$, tous ses diviseurs le sont aussi (*cf.* le lemme 5.3.5). *q.e.d.*

# Chapitre 6

# Décomposition spectrale

Soient $E = \mathbb{K}-$espace vectoriel de dimension finie et $u \in \mathscr{L}(E)$.
**Objectif :** (si $E$ est de dimension finie) construire une base $\mathscr{B}$ telle que :

$$\mathrm{Mat}(u)_{\mathscr{B}} = \begin{pmatrix} T_1 & & & \\ & T_2 & & \\ & & \ddots & \\ & & & T_p \end{pmatrix}$$

où les $T_i$ sont des blocs triangulaires supérieures avec diagonale constante.

## 6.1 Sous-espaces caractéristiques

**Définition 48** *Soit $\lambda \in \mathbb{K}$. Un vecteur propre généralisé de $u$ de poids $\lambda$ est un vecteur $v \in E$ tel que :*

$$(u - \lambda \mathrm{Id}_E)^m v = 0$$

*pour un certain entier $m \geq 0$. Le plus petit entier $m$ de la sorte est appelé la hauteur de $v$.*

En particulier, les vecteurs propres sont des vecteurs propres généralisés de hauteur 1. Il est bien pratique de considérer le vecteur nul comme un vecteur propre généralisé de hauteur 0 pour tout $\lambda \in \mathbb{K}$.

Exemple : Soit $E := \mathscr{C}^\infty(\mathbb{R})$ le $\mathbb{R}-$espace vectoriel des fonctions réelles infiniment dérivables. Considérons l'endomorphisme de dérivation $u := D : E \to E$, $f \mapsto f'$. Les vecteurs propres associés à $\lambda \in \mathbb{R}$ sont les fonctions (non nulles) proportionnelles à $e^{\lambda x}$ et les vecteurs propres généralisés sont

les fonctions de la forme $p(x)e^{\lambda x}$ pour un certain polynôme $p(x)$ (en effet, si $f = e^{\lambda x}g$, alors :

$$(D - \lambda \mathrm{Id}_E)^m(f) = e^{\lambda x}g^{(m)} = 0 \Leftrightarrow g^{(m)} = 0$$

$$\Leftrightarrow g \text{ est un polynôme de degré } \leq m-1 \ .$$

La hauteur d'une telle fonction $e^{\lambda x}p(x)$ est $\deg p + 1$. En particulier, les polynômes sont les vecteurs propres généralisés associés à 0.

**Remarque :**

Si $v$ est un vecteur propre généralisé de hauteur $m$ associé à $\lambda \in \mathbb{K}$, alors

$$(u - \lambda \mathrm{Id}_E)^{m-1}v$$

est un vecteur propre de poids (*c-à-d* de valeur propre) $\lambda$. Donc $\lambda$ est une racine du polynôme caractéristique (si $E$ est de dimension finie).

**Exercice 43 (important)** *L'ensemble des vecteurs propres généralisés de poids $\lambda$ et de hauteur $\leq m$ est un sous-espace de $E$, stable par $u$ : c'est exactement* $\ker(u - \lambda \mathrm{Id}_E)^m$.

On a une chaîne croissante de sous-espaces stables :

$$\ker(u - \lambda \mathrm{Id}_E) \subseteq \ker(u - \lambda \mathrm{Id}_E)^2 \subseteq ...$$

**Définition 49** *Soit $\lambda \in \mathbb{K}$. Le sous-espace caractéristique de $u$ de poids $\lambda$ est la réunion :*

$$E^\lambda(u) := \cup_{n=1}^\infty \ker(u - \lambda \mathrm{Id}_E)^n$$

*c-à-d :*

$$E^\lambda(u) = \{v \in E \ : \ ^\exists m \geq 0, \ (u - \lambda \mathrm{Id}_E)^m(v) = 0\}$$

*c'est un sous-espace de $E$ stable par $u$.*

**Remarque :**

La suite des dimensions est croissante :

$$\dim \ker(u - \lambda \mathrm{Id}_E) \leq \dim \ker(u - \lambda \mathrm{Id}_E)^2 \leq ...$$

En dimension finie, cette suite est stationnaire donc il existe un entier $m$ tel que : $E^\lambda(u) = \ker(u - \lambda \mathrm{Id}_E)^m$.

Nous allons maintenant voir pourquoi cette notion de sous-espace caractéristique est importante.

Rappelons que pour tout $\lambda$, le sous-espace $E^\lambda(u)$ est stable par $u$ et donc par tout polynôme en $u$.

**Lemme 6.1.1** *i) Si* $\dim E^\lambda(u) < \infty$*, alors il existe une base de* $E^\lambda(u)$ *où la matrice de la restriction* $u\big|_{E^\lambda(u)}$ *est triangulaire supérieure avec* $\lambda$ *sur la diagonale :*

$$\begin{pmatrix} \lambda & & \cdots \\ & \ddots & \vdots \\ & & \lambda \end{pmatrix} .$$

*ii) Pour tous* $\mu \neq \lambda$*,* $(u - \mu \mathrm{Id}_E)^m$ *est injectif sur* $E^\lambda(u)$*.*

*Démonstration* : i) Soit $k := \dim(E^\lambda)$.
Notons $V_i := \ker(u - \lambda \mathrm{Id}_E)^i$ pour tout $i \geq 0$. (Donc $V_0 = \{0\}$).
Soit $m \geq 0$ le plus petit entier tel que $V_m = V_{m+1}$ ; Alors :

$$0 = V_0 \underset{\neq}{\subseteq} V_1 \underset{\neq}{\subseteq} ... \underset{\neq}{\subseteq} V_m = V_{m+1}$$

de plus :

$$v \in V_{m+2} \Leftrightarrow (u - \lambda \mathrm{Id}_E)^{m+2} v = 0$$
$$\Leftrightarrow (u - \lambda \mathrm{Id}_E) v \in V_{m+1}$$
$$\Leftrightarrow (u - \lambda \mathrm{Id}_E) v \in V_m$$
$$\Leftrightarrow v \in V_{m+1}$$

donc $V_m = V_{m+1} = V_{m+2} = V_{m+3} = ... = E^\lambda$.

Soit $e_1, ..., e_{k_1}$ une base de $V_1 = \ker(u - \lambda \mathrm{Id}_E)$ que l'on complète en une base $e_1, ..., e_{k_2}$ de $V_2 = \ker(u - \lambda \mathrm{Id}_E)^2$, que l'on complète en ......etc, que l'on complète en $e_1, ..., e_{k_m}$ une base de $E^\lambda$.

On a alors : $k_1 < k_2 < ... < k_m = k$ et pour tout $0 \leq i \leq m$ :

$$V_i = \langle e_1, ..., e_{k_i} \rangle \ .$$

Or pour tout $i \geq 1$ :

$$(u - \lambda \mathrm{Id}_E)(V_i) \subseteq V_{i-1}$$

en particulier,

$$^\forall k_{i-1} < j \leq k_i,\ u(e_j) = \lambda e_j \mod \langle e_1, ..., e_{k_{i-1}} \rangle$$

et la matrice de la restriction

$$u|_{E^\lambda}$$

dans la base $e_1, ...e_{k_m}$ est triangulaire de la forme :

$$B = \begin{pmatrix} \lambda & & \cdots \\ & \ddots & \vdots \\ & & \lambda \end{pmatrix} .$$

ii) Il suffit de montrer que $(u - \mu \mathrm{Id}_E)$ est injectif sur $E^\lambda(u)$ *c-à-d* :

$$\ker(u - \mu \mathrm{Id}_E) \cap E^\lambda(u) = 0$$

or, si $(u - \mu \mathrm{Id}_E)(x) = 0$ et $x \in E^\lambda(u)$, alors :

$$\begin{aligned}(u - \lambda \mathrm{Id}_E)(x) &= (u - \mu \mathrm{Id}_E)(x) + (\mu - \lambda)x \\ &= (\mu - \lambda)x \\ \forall l \geq 0,\ (u - \lambda \mathrm{Id}_E)^l(x) &= (\mu - \lambda)^l x \\ &\Rightarrow (\mu - \lambda)^l x = 0\end{aligned}$$

pour $l$ assez grand car $x \in E^\lambda(u)$. Donc $x = 0$, car $\mu \neq \lambda$. *q.e.d.*

**Proposition 6.1.2** *Si $E$ est de dimension finie, alors le sous-espace caractéristique de $u$ de poids $\lambda$ est de dimension la multiplicité de $\lambda$ dans le polynôme caractéristique $\chi_u(X)$ :*

$$\dim E^\lambda(u) = m_a(\lambda) \ .$$

*Démonstration* : Soit $e_1, ..., e_k$ une base de $E^\lambda(u) =: E^\lambda$ où la matrice de la restriction $u\big|_{E^\lambda(u)}$ est de la forme :

$$B = \begin{pmatrix} \lambda & \cdots & \vdots \\ & \ddots & \vdots \\ & & \lambda \end{pmatrix} \ .$$

Donc $\chi_{u|_{E^\lambda}}(X) = (X - \lambda)^k$.

On complète la base $e_1, ..., e_k$ en :

$$e_1, ..., e_k, e_{k+1}, ..., e_n$$

une base de $E$.

Remarquons que $E^\lambda$ est stable par $u$ en effet :

$$(u - \lambda \mathrm{Id}_E)^m(v) = 0 \Rightarrow (u - \lambda \mathrm{Id}_E)^m.u(v) = u.(u - \lambda \mathrm{Id}_E)^m(v) = 0 \ .$$

Dans cette base, la matrice de $u$ est de la forme :

$$\left(\begin{array}{c|c} B & ? \\ \hline 0 & D \end{array}\right)$$

où $D \in \mathscr{M}_{n-k}(\mathbb{K})$.

Donc :

$$\chi_u(X) = (X-\lambda)^k \chi_D(X)$$

il reste donc à montrer que $\chi_D(\lambda) \neq 0$. Sinon, il existerait $0 \neq w \in \langle e_{k+1}, ..., e_n \rangle$ tel que : $Dw = \lambda w$.

Mais alors :

$$u(w) = \lambda w + y$$

avec $y \in E^\lambda$. Donc :

$$\begin{aligned}(u - \lambda \mathrm{Id}_E)w \in E^\lambda = \ker(u-\lambda\mathrm{Id}_E)^m \\ \Rightarrow (u-\lambda\mathrm{Id}_E)^{m+1} w = 0 \\ \Rightarrow w \in E^\lambda \cap \langle e_{k+1}, ..., e_n \rangle \\ \Rightarrow w = 0\end{aligned}$$

contradiction ! *q.e.d.*

**Proposition 6.1.3** *Les sous-espaces caractéristiques de poids distincts* $\lambda_1, ..., \lambda_r$ *sont en somme directe*

*Démonstration :* Soient $v_1, ..., v_r$ tels que :

$$v_1 + ... + v_r = 0$$

et $v_i \in E^{\lambda_i}$ pour tout $i$.

Pour tout $i$, il existe un entier $k_i$ tel que :

$$v_i \in \ker(u - \lambda_i \mathrm{Id}_E)^{k_i}$$

il suffit donc de vérifier que les polynômes $(X - \lambda_i)^{k_i}$ sont deux à deux premiers entre eux car alors : les sous-espaces $\ker(u - \lambda_i \mathrm{Id}_E)^{k_i}$ sont en somme directe d'après le lemme des noyaux et $v_1 = ... = v_r = 0$. Nous allons montrer que $P(X) = (X-\lambda)^m$, $Q(X) = (X-\mu)^n$, $m, n$ entiers $\geq 1$, $\lambda \neq \mu \in \mathbb{K}$ sont premiers entre eux. Soit $c := \frac{1}{\mu - \lambda}$. On a :

$$1 = c((X-\lambda) - (X-\mu))$$

en élevant à la puissance $m+n-1$ :

$$1 = c^{m+n-1}(r(X)(X-\lambda)^m + s(X)(X-\mu)^n)$$

pour certains polynômes $r(X), s(X) \in \mathbb{K}[X]$ de degrés respectifs $\leq n-1$ et $\leq m-1$ (*exo*) (utiliser la formule du binôme). Donc, $P(X)$ et $Q(X)$ sont premiers entre eux. *q.e.d.*

**Théorème 6.1.4** *Supposons $E$ de dimension finie. Si le polynôme caractéristique de $u$ est scindé sur $\mathbb{K}$, alors :*

$$E = \oplus_{i=1}^{r} E^{\lambda_i}$$

*où $\lambda_1, ..., \lambda_r$ sont les racines distinctes de $\chi_u(X)$.*

*Démonstration :* On a déjà vu que la somme est directe. Si $\chi_u(X) = (X - \lambda_1)^{m_1} ... (X - \lambda_r)^{m_r}$, alors d'après le théorème de Cayley-Hamilton, $\chi_u(u) = 0$ donc :

$$E = \oplus_i \ker(u - \lambda_i \mathrm{Id}_E)^{m_i} \subseteq \oplus_i E^{\lambda_i} \quad .$$

*q.e.d.*

## Interprétation géométrique des multiplicités du polynôme minimal

Supposons que $E$ est de dimension finie et que le polynôme caractéristique de $u$ est scindé sur $\mathbb{K}$. Alors, comme le polynôme minimal $m_u(X)$ de $u$ divise $\chi_u(X)$, $m_u(X)$ est aussi scindé sur $\mathbb{K}$. Factorisons-le :

$$m_u(X) = (X - \lambda_1)^{k_1} ... (X - \lambda_r)^{k_r}$$

pour certains $\lambda_1, ..., \lambda_r \in \mathbb{K}$ deux à deux distincts et certains entiers $k_i \geq 1$.

**Théorème 6.1.5** *Pour tout $1 \leq i \leq r$, $k_i$ est aussi le plus petit entier $m$ tel que*

$$\ker(u - \lambda_i \mathrm{Id}_E)^m = \ker(u - \lambda_i \mathrm{Id}_E)^{m+1} (= E^{\lambda_i})$$

*Démonstration :* Notons $m_i$ le plus petit entier $m$ tel que

$$\ker(u - \lambda_i \mathrm{Id}_E)^m = \ker(u - \lambda_i \mathrm{Id}_E)^{m+1} ,$$

pour tout $i$. Alors :

$$E = \oplus_i E^{\lambda_i} = \oplus_i (\ker(u - \lambda_i \mathrm{Id}_E)^{m_i})$$

donc :

$$(u - \lambda_1 \mathrm{Id}_E)^{m_1} ... (u - \lambda_r \mathrm{Id}_E)^{m_r} = 0$$

et le polynôme $(X - \lambda_1)^{m_1} ... (X - \lambda_r)^{m_r}$ annule $u$ donc :

$$m_u(X) \text{ divise } (X - \lambda_1)^{m_1} ... (X - \lambda_r)^{m_r}$$

et $k_i \leq m_i$ pour tout $i$.

D'un autre côté, $m_u(u) = 0 \Rightarrow$

$$\bigoplus_{i=1}^{r} \ker(u - \lambda_i \mathrm{Id}_E)^{k_i} = E \quad .$$

Soit $x \in E^{\lambda_i}$. Il existe $x_1 \in \ker(u - \lambda_1)^{k_1}, ..., x_r \in \ker(u - \lambda_r)^{k_r}$ tels que :

$$x = x_1 + ... + x_r$$

$$\Rightarrow x - x_i \in E^{\lambda_i} \cap \left( \oplus_{\substack{j=1 \\ j \neq i}}^{r} \ker(u - \lambda_j \mathrm{Id}_E)^{k_j} \right)$$

$$\subseteq E^{\lambda_i} \cap \left( \oplus_{\substack{j=1 \\ j \neq i}}^{r} E^{\lambda_j} \right) = \{0\}$$

Donc $x = x_i \in \ker(u - \lambda_i \mathrm{Id}_E)^{k_i}$. D'où :

$$E^{\lambda_i} = \ker(u - \lambda_i \mathrm{Id}_E)^{m_i} \subseteq \ker(u - \lambda_i \mathrm{Id}_E)^{k_i}$$

et donc $k_i \geq m_i$. *q.e.d.*

## 6.2 Projecteurs spectraux

Supposons $E$ de dimension finie $n$ et le polynôme $\chi_u(X)$ scindé sur $\mathbb{K}$ :

$$\chi_u = (X - \lambda_1)^{m_1} ... (X - \lambda_r)^{m_r}$$

avec $\lambda_i \in \mathbb{K}$ deux à deux distincts, $1 \leq m_i$ et $m_1 + ... m_r = n$. Rappelons que

$$E = \oplus_{i=1}^{r} E^{\lambda_i} \quad .$$

**Définition 50** *Pour toute valeur propre $\lambda_i$, on note $\pi_{\lambda_i}$ ou $\pi_i$ la projection sur le sous-espace $E^{\lambda_i}$ parallèlement au sous-espace :*

$$\oplus_{\substack{j=1 \\ j \neq i}}^{r} E^{\lambda_j}$$

*autrement dit si $x = x_1 + ... + x_r$ où chaque $x_i \in E^{\lambda_i}$, $\pi_i(x) = x_i$, autrement dit (encore) :*

$$\pi_i(x) = x \text{ si } x \in E^{\lambda_i} \text{ et } 0 \text{ si } x \in E^{\lambda_j},\ i \neq j.$$

*Les $\pi_i$ sont les projecteurs spectraux de $u$.*

**Propriétés :**
— les $\pi_i$ sont linéaires ;
— $\pi_1 + ... + \pi_r = \mathrm{Id}_E$ ;
— $^\forall i \neq j,\ \pi_i \pi_j = 0$ ;
— $^\forall i, \pi_i^2 = \pi_i$ ;
— $\mathrm{Im}\,\pi_i = E^{\lambda_i}$ ;
— $\ker \pi_i = \bigoplus_{\substack{1 \le j \le r \\ j \neq i}} E^{\lambda_j}$.

**Remarque :** Si $m_u(X) = (X-\lambda_1)^{k_1}...(X-\lambda_r)^{k_r}$, alors

$$E^{\lambda_i} = \ker(u - \lambda_i \mathrm{Id}_E)^{k_i}$$

pour tout $i$.

**Proposition 6.2.1** *Les projecteurs spectraux sont des polynômes en $u$.*

*Démonstration* : En effet, soit $1 \le i \le r$. Posons :

$$Q_i(X) := \frac{m_u(X)}{(X-\lambda_i)^{k_i}} = \prod_{\substack{j=1 \\ j \neq i}}^{r} (X-\lambda_j)^{k_j} \in \mathbb{K}[X] \ .$$

Comme $Q_i(\lambda_i) \neq 0$,

$$Q_i(X) = a_0 + a_1(X-\lambda_i) + a_2(X-\lambda_i)^2 + ...$$

pour certains coefficients $a_0, a_1, a_2, ... \in \mathbb{K}$ tels que $a_0 \neq 0$. On peut alors trouver

$$U_i(X) = b_0 + b_1(X-\lambda_i) + ... + b_{k_i-1}(X-\lambda_i)^{k_i-1} \in \mathbb{K}[X]$$

un polynôme de degré $< k_i$ tel que :

$$1 = (a_0+a_1(X-\lambda_i)+a_2(X-\lambda_i)^2+...)(b_0+b_1(X-\lambda_i)+...+b_{k_i-1}(X-\lambda_i)^{k_i-1}) \bmod (X-\lambda_i)^{k_i}$$

$$\textit{c-à-d} \ : 1 = Q_i(X)U_i(X) \bmod (X-\lambda_i)^{k_i} \ .$$

Il suffit alors de remarquer que :

$$\pi_i = (U_i Q_i)(u)$$

en effet :

$$\text{si } x \in E^{\lambda_i} = \ker(u-\lambda_i \mathrm{Id}_E)^{k_i}, \text{ alors } (U_iQ_i)(u)(x) = \mathrm{Id}_E(x) = x$$

$$\text{si } x \in E^{\lambda_j} = \ker(u-\lambda_j \mathrm{Id}_E)^{k_j},\ j \neq i, \text{ alors } (U_iQ_i)(u)(x) = 0 \ .$$

**Remarque :** Le polynôme $1 - U_1(X)Q_1(X) - ... - U_r(X)Q_r(X)$ est de degré $< k_1 + ... + k_r$. Or, pour tout $i$, la multiplicité de $\lambda_i$ dans le polynôme :

$$1 - U_1(X)Q_1(X) - ... - U_r(X)Q_r(X)$$

est $\geq k_i$ (car si $j \neq i$, $(X - \lambda_i)^{k_i}$ divise $Q_j(X)$), donc :

$$0 = 1 - U_1(X)Q_1(X) - ... - U_r(X)Q_r(X)$$

$$\Leftrightarrow 1 = U_1(X)Q_1(X) + ... + U_r(X)Q_r(X)$$

$$\Leftrightarrow \frac{1}{m_u(X)} = \frac{U_1(X)}{(X - \lambda_1)^{k_1}} + ... + \frac{U_r(X)}{(X - \lambda_1)^{k_r}} \ .$$

*q.e.d.*

## 6.3 Décomposition de Dunford-Jordan

Un endomorphisme $N$ de $E$ est nilpotent si $N^k = 0$ pour un certain $k \geq 0$.

**Théorème 6.3.1** *Soit $u \in \mathscr{L}(E)$ tel que $\chi_u$ est scindé sur $\mathbb{K}$. Alors il existe un unique couple $(d, n)$ tels que :*
*0) $d, n \in \mathscr{L}(E)$ ;*
*i) $d$ diagonalisable, $n$ nilpotent ;*
*ii) $dn = nd$ ;*
*iii) $u = d + n$.*
*De plus, $d, n$ sont des polynômes en $u$.*

Cette décomposition

$$u = d + n$$

est appelée décomposition de Dunford-Jordan.

**Remarque :** Même énoncé avec une matrice $A$ à la place de $u$.

*Démonstration :*
soient $\pi_i$ les projecteurs spectraux de $u$.
— **existence :** $d := \lambda_1\pi_1 + ... + \lambda_r\pi_r$, $n := u - d$.
Pour tout $x \in E^{\lambda_i}$, $d(x) = \lambda_i x$. Donc

$$E^{\lambda_i} \subseteq \ker(d - \lambda_i \mathrm{Id}_E)$$

et :

$$E = \oplus_i \ker(d - \lambda_i \mathrm{Id}_E)$$

et $d$ est diagonalisable avec les mêmes valeurs propres que $u$.

Pour tout $x \in E^{\lambda_i}$,

$$\begin{aligned} n(x) &= u(x) - d(x) \\ &= (u - \lambda_i \mathrm{Id}_E)(x) \end{aligned}$$

et par récurrence :

$$n^k(x) = (u - \lambda_i)^k(x) \ .$$

Donc si $k \geq \max_{1 \leq i \leq r} \{k_i\}$, $n^k(x) = 0$.

On a construit $d$ et $n$ comme des polynômes en $u$ ce qui est important pour la suite.

**Lemme 6.3.2** *Soit $(d_\alpha)_{\alpha \in \mathscr{A}}$ une famille d'endomorphismes de $E$ diagonalisables qui commutent deux à deux. Si $E$ est de dimension finie alors il existe une base commune de diagonalisation.*

*Démonstration :* Si tous les $d_\alpha$ sont des homothéties, c'est évident. Sinon on raisonne par récurrence sur $\dim E$ et on choisit un $d_{\alpha_0}$ qui n'est pas une homothétie. Soient $\lambda_1, ..., \lambda_r$ ses valeurs propres distinctes. Alors pour tout $i$, $V_i := \ker(d_{\alpha_0} - \lambda_i)$ est un sous-espace de $E$ de dimension $< \dim E$ (car $d_{\alpha_0}$ n'est pas une homothétie) et chaque $V_i$ est stable par $d_\alpha$ pour tout $\alpha$ (car $d_\alpha d_{\alpha_0} = d_{\alpha_0} d_\alpha$). Par hypothèse de récurrence il existe une base $\mathscr{B}_i$ de $V_i$ formée de vecteurs propres communs à tous les $d_\alpha$. La réunion :

$$\mathscr{B}_1 \cup ... \cup \mathscr{B}_r$$

est alors une base de $V_1 \oplus ... \oplus V_r = E$, une base de diagonalisation pour tous les $d_\alpha$. *q.e.d.*

— **unicité :** supposons que $u = d' + n'$ avec $d'$ diagonalisable, $n'$ nilpotent et $d'n' = n'd'$. Alors : $d' - d = n - n'$. Or $n'$ commute avec $d'$ et $n'$ donc avec $u = d' + n'$ et avec $n$ qui est un polynôme en $u$. On en déduit que $n' - n$ est nilpotent (*exo*) .

De même, $d'$ commute avec $u$ donc $d'$ laisse stable chaque $E^{\lambda_i} = \ker(u - \lambda_i \mathrm{Id}_E)^{k_i}$. Mais alors

$$d'|_{E^{\lambda_i}}$$

est diagonalisable et :

$$(d' - d)|_{E^{\lambda_i}} = (d' - \lambda_i \mathrm{Id}_E)|_{E^{\lambda_i}}$$

est diagonalisable et nilpotent donc nul (nilpotent $\Rightarrow$ la seule valeur propre est $O$ et diagonalisable avec pour seule valeur propre 0 $\Rightarrow$ nul). Donc $d' = d$ sur chaque $E^{\lambda_i}$, comme $E = \oplus_i E^{\lambda_i}$, par linéarité, $d' = d$. On a aussi : $n' = u - d' = u - d = n$.

*q.e.d.*

**À retenir :**

— $d = \lambda_1\pi_1 + ...\lambda_r\pi_r$ et les valeurs propres de $u$ sont les valeurs propres de $d$.

— diagonalisable et nilpotent $\Rightarrow$ nul.

**Exercice 44** $\chi_u(X) = \chi_d(X)$.

**Proposition 6.3.3** *$u$ diagonalisable $\Leftrightarrow u = d$ ssi $n = 0$ ;*
*$u$ nilpotent $\Leftrightarrow u = n$ ssi $d = 0$.*

*Démonstration :* C'est une conséquence directe de la décomposition de Dunford-Jordan. *q.e.d.*

Exemple :

— si $A = \begin{pmatrix} \lambda & \cdots & \\ & \ddots & \vdots \\ & & \lambda \end{pmatrix}$, $D = \lambda I_n$ et $N = \begin{pmatrix} 0 & \cdots & \\ & \ddots & \vdots \\ & & 0 \end{pmatrix}$ ;

— **ATTENTION !** si $u = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}$, $d = u$, $n = 0$.

## 6.4 Calcul pratique des projecteurs spectraux

### 6.4.1 Méthode

Soit $u \in \mathscr{L}(E)$. Supposons que $Q \neq 0$ est un polynôme annulateur de $u$ scindé sur $\mathbb{K}$ (en particulier $\chi_u$ est scindé !) (Plus le degré de $Q$ est bas moins compliqués sont les calculs).

**1ère étape :** Factoriser $Q$ :

$$Q = (X - \lambda_1)^{l_1}...(X - \lambda_r)^{l_r}$$

$\lambda_i$ deux à deux $\neq$ et $l_i \geq 1$.

**2ème étape :** Décomposer $\frac{1}{Q}$ en éléments simples :

$$(*)\quad \frac{1}{Q} = \frac{R_1(X)}{(X - \lambda_1)^{l_1}} + ...$$

où $R_i(X)$ : polynômes de degré $< l_i$ (une telle décomposition est unique).

**3ème étape :** $\pi_{\lambda_i} = R_i(u)Q_i(u)$ où $Q_i(X) := \frac{Q(X)}{(X-\lambda_i)^{l_i}} = \prod_{\substack{1\leq j\leq r \\ j\neq i}} (X - \lambda_j)^{l_j}$.

**justification :** la décomposition $(*)$ multipliée par $Q$ donne une relation de Bézout :

$$1 = R_i(X)Q_i(X) + (X - \lambda_i)^{l_i} S(X)$$

pour un certain polynôme $S(X)$.

### 6.4.2 Exemples

a) cas où $u$ diagonalisable avec seulement 2 valeurs propres :
si

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

alors on sait que $A$ est diagonalisable et que ses valeurs propres sont $0, 3$. Les projecteurs spectraux associés $\pi_0$, $\pi_1$ vérifient :

$$\pi_0 + \pi_3 = I_3 \text{ et } 3\pi_3 = D = A$$

donc :

$$\pi_3 = \frac{1}{3}A \text{ et } \pi_0 = I_3 - \frac{1}{3}A$$

b)

$$A := \begin{pmatrix} 1 & 0 & -3 \\ 1 & -1 & -6 \\ -1 & 2 & 5 \end{pmatrix}$$

$$\chi_A(X) = m_A(X) = (X-1)(X-2)^2$$

$$\frac{1}{m_A(X)} = \frac{1}{X-1} + \frac{3-X}{(X-2)^2}$$

$$\Leftrightarrow 1 = \frac{m_A(X)}{X-1} + \frac{m_A(X)(3-X)}{(X-2)^2}$$

donc :

$$\pi_1 = \left(\frac{m_A(X)}{X-1}\right)(A) = (A-2I_3)^2 \text{ et } \pi_2 = \left(\frac{m_A(X)(3-X)}{(X-2)^2}\right)(A) = -A^2+4A-3I_3.$$

# 6.5 Réduction de Jordan

Nous allons montrer que toute matrice dont le polynôme caractéristique est scindé est semblable à une matrice diagonale par blocs avec des blocs « presque » diagonaux.

## 6.5.1 Blocs de Jordan

**Définition 51** *Un bloc de Jordan est une matrice de la forme :*

$$J_{\lambda,n} := \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix} \in \mathscr{M}_n(\mathbb{K})$$

*où* $\lambda \in \mathbb{K}, n \geq 0$.

On a :

$$(J_{\lambda,n} - \lambda I_n)^k = \begin{pmatrix} 0 & \cdots & \overset{k}{0} & 1 & 0 & \cdots & 0 \\ \vdots & & & \ddots & \ddots & & \vdots \\ \vdots & & & & \ddots & \ddots & \vdots \\ \vdots & & & & & \ddots & 1 \\ \vdots & & & & & & 0 \\ \vdots & & & & & & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \end{pmatrix} \text{ si } 0 \leq k \leq n-1$$

$$\text{et } (J_{\lambda,n} - \lambda I_n)^k = 0 \text{ si } n < k.$$

On a aussi $J_{\lambda,n} - \mu I_n$ inversible si $\mu \neq \lambda$.

**Exercice 45** *Le polynôme caractéristique et le polynôme minimal d'un bloc de Jordan sont égaux à* $(X - \lambda)^n$.

**Définition 52** *Une matrice de Jordan est une matrice diagonale par blocs de la forme :*

$$\begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_r \end{pmatrix}$$

*où les* $J_i$ *sont des blocs de Jordan.*

**Exercice 46** *Une matrice de Jordan est diagonalisable si et seulement si ses blocs sont tous de taille* 1.

### 6.5.2 Matrices nilpotentes

Supposons que $E$ est un $\mathbb{K}-$espace vectoriel de dimension $n$. Soit $u$ un endomorphisme de $E$.

**Définition 53** *Soit $e \in E$. On appelle hauteur de $e$, notée $h(e)$, le plus petit entier $m \geq 0$ tel que $u^m(e) = 0$.*

**Lemme 6.5.1** *Si $e \in E$ un vecteur de hauteur $m$. Alors*

$$e, u(e), ..., u^{m-1}(e)$$

*sont linéairement indépendants.*

*Démonstration :* Supposons que

$$\lambda_0 e + ... + \lambda_{m-1} u^{m-1}(e) = 0$$

et que $\lambda_k$ est le premier coefficient $\neq 0$, $0 \leq k \leq m-1$. Alors si on allique $u^{m-k-1}$, on trouve :

$$\lambda_k u^{m-1}(e) = 0$$
$$\Rightarrow \lambda_k = 0$$

car $u^{m-1}(e) \neq 0$ *absurdo.* *q.e.d.*



**Corollaire 6.5.1.1** *On a forcément, $u^{\dim E} = 0$ pour tout endomorphisme nilpotent de $E$.*

**Définition 54** *On dit que le sous-espace $\langle e, u(e), ..., u^{m-1}(e)\rangle$ est le sous-espace cyclique de $u$ engendré par $e$.*

Un sous-espace cyclique est invariant par $u$ (*exo*) et la restriction de de $u$ au sous-espace cyclique :

$$\langle e, u(e), ..., u^{m-1}(e)\rangle$$

a pour matrice

$$J_{0,n} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & 0 \end{pmatrix} \in \mathscr{M}_n(\mathbb{K})$$

dans la base

$$u^{m-1}(e), ..., u(e), e \ .$$

**Remarque :** [importante] Soit $e$ un vecteur de hauteur $m$. Un vecteur $x$ du sous-espace cyclique

$$\langle e, u(e), ..., u^{m-1}(e)\rangle$$

qui n'est pas dans l'image de $u$ est de hauteur $m$.

En effet, si

$$x = \lambda_0 e + ... + \lambda_{m-1} u^{m-1}(e)$$

avec $\lambda_0 \neq 0$, $u^m(x) = 0$ et $u^{m-1}(x) = \lambda_0 u^{m-1}(e) \neq 0$.

**Théorème 6.5.2** *L'espace $E$ est une* **somme directe** *de sous-espaces cycliques de l'opérateur $u$ :*

$$E = E_1 \oplus ... \oplus E_r \ .$$

*En particulier, il existe une base de $E$ où la matrice de $u$ est une matrice de Jordan de la forme :*

$$\left(\begin{array}{c|c|c} J_{0,n_1} & & \\ \hline & \ddots & \\ \hline & & J_{0,n_r} \end{array}\right) .$$

*Et le nombre $r$ de composantes est $r = \dim \ker u$*

*Démonstration :* Supposons que $E$ est une somme directe de sous-espaces cycliques

$$E_i = \langle e_i, ..., u^{n_i-1}(e_i)\rangle$$

alors, la matrice de $u$ dans la base :

$$u^{n_1-1}(e_1), ..., e_1, u^{n_2-1}(e_2), ..., e_2, ..., u^{n_r-1}(e_r), ..., e_r$$

est de la forme

$$\left(\begin{array}{c|c|c} J_{0,n_1} & & \\ \hline & \ddots & \\ \hline & & J_{0,n_r} \end{array}\right)$$

donc :

$$\mathrm{rang} u = \mathrm{rang} J_{0,n_1} + ... + \mathrm{rang} J_{0,n_r}$$

$$(n_1 - 1) + ... + (n_r - 1) = \dim E - r$$

$$\Leftrightarrow r = \dim E - \text{rang} u = \dim \ker u \ .$$

Démontrons par récurrence sur $n = \dim E \geq 0$ que $E$ est une somme directe de sous-espaces cycliques. Si $n = 0$, il n'y a rien à montrer. Supposons que $n > 0$.

Comme $u$ n'est pas surjective (*exo*) , il existe un sous-espace de $E$, disons $H$, de dimension $n - 1$ tel que :

$$\text{Im}\, u \subseteq H \ .$$

Ce $H$ est stable par $u$. Par hypothèse de récurrence,

$$H = H_1 \oplus ... \oplus H_r$$

où les $H_i$ sont des sous-espaces cycliques de $u|_H$ (donc de $u$). On choisit un vecteur $e \in E \setminus H$.

On a :

$$u(e) = u_1 + ... + u_r \ , {}^{\forall} i, \ u_i \in H_i \ .$$

Si pour un certain $i$, $u_i = u(v_i)$, avec $v_i \in H_i$, alors on remplace $e$ par $e - v_i \in E \setminus H$. On peut donc supposer que pour tout $i = 1$ à $r$, $u_i = 0$ ou $u_i \in H_i \setminus u(H_i)$. C'est-à-dire : $u_i = 0$ ou $H_i$ est cyclique engendré par $u_i$.

Si $u(e) = 0$, alors :

$$E = \mathbb{K}e \oplus H_1 \oplus ... \oplus H_r$$

est une décomposition de $E$ en sous-espaces cycliques.

Si $u(e) \neq 0$, alors :

$$0 < h(u(e)) = \max_i h(u_i)(exo) \ .$$

Quitte à renuméroter, on peut supposer que

$$h(u(e)) = h(u_1) =: m \ .$$

Mais alors : $h(e) = m + 1$. Vérifions que

$$E = \langle e, u(e), ..., u^m(e) \rangle \oplus H_2 \oplus ... \oplus H_r \ .$$

Comme $h(u_1) = \dim H_1 = m$, on a :

$$\dim E = \dim H + 1 = (m + 1) + \dim H_2 + ... + \dim H_r$$

et il suffit de démontrer que

$$\langle e, ..., u^m(e) \rangle \cap (H_2 \oplus ... \oplus H_r) = 0 \ .$$

Si $\lambda_0 e + ... + \lambda_m u^m(e) \in H_2 \oplus ... \oplus H_r$, alors, comme $e \notin \mathrm{Im}\, u$, $\lambda_0 = 0$.
Or, $u(e) = u_1 + ... + u_r$ donc :

$$\lambda_1 u(e) + ... + \lambda_m u^m(e) = \lambda_1 u_1 + ... + \lambda_m u^{m-1}(u_1) \bmod H_2 \oplus ... \oplus H_r$$

$$\Rightarrow \lambda_1 u_1 + ... + \lambda_m u^{m-1}(u_1) \in H_1 \cap (H_2 \oplus ... \oplus H_r) = 0$$

$$\Rightarrow \lambda_1 = ... = \lambda_m = 0$$

car $h(u_1) = m$. *q.e.d.*

### 6.5.3 Réduction de Jordan

**Théorème 6.5.3** *Soit $u$ un endomorphisme de $E$ dont le polynôme caractéristique, $\chi_u(X)$ est* **scindé** *sur $\mathbb{K}$.*

*Existence : il existe une base de $E$ où la matrice de $u$ est de Jordan* i.e. *:*

$$\mathrm{Mat}(u) = \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_r \end{pmatrix}$$

*où les $J_i$ sont des blocs de Jordan.*

*Version matricielle : si $A \in \mathscr{M}_n(\mathbb{K})$ a son polynôme caractéristique scindé sur $\mathbb{K}$, alors, $A$ est semblable (sur $\mathbb{K}$) à une matrice de Jordan.*

*Unicité : le nombre de blocs de Jordan de la forme $J_{\lambda,m}$ noté :*

$$^\forall \lambda \in \mathbb{K}, {}^\forall m \geq 1,\ N_{\lambda,m} := \{1 \leq i \leq r\ :\ J_i = J_{\lambda,m}\}$$

*ne dépend que de $u$ (ou de $A$) :*

*les $\lambda$ qui apparaissent sont les valeurs propres de $u$ (ou de $A$) et plus précisément, on a :*

$$N_{\lambda,m} = \mathrm{rg}\,(u - \lambda \mathrm{Id}_E)^{m+1} - 2\mathrm{rg}\,(u - \lambda \mathrm{Id}_E)^m + \mathrm{rg}\,(u - \lambda \mathrm{Id}_E)^{m-1}$$

*pour tout $\lambda \in \mathbb{K}$ et tout $m \geq 1$.*

**Remarque :** En particulier, ce théorème s'applique à TOUTES les matrices complexes.

*Démonstration* : Existence : notons $E^{\lambda_1}, ..., E^{\lambda_r}$ les sous-espaces propres généralisés de $u$. Alors chaque $E^{\lambda_i}$ est stable par $u$ et $E$ se décompose en :

$$E = E^{\lambda_1} \oplus ... \oplus E^{\lambda_r}\ .$$

De plus , pour tout $i$,

$$u|_{E^{\lambda_i}} - \lambda_i \mathrm{Id}_{E^{\lambda_i}}$$

est nilpotent. On peut donc appliquer le théorème 6.5.2 à $u|_{E^{\lambda_i}} - \lambda_i \mathrm{Id}_{E^{\lambda_i}}$ pour tout $i$. Et on remarque que :

$$\left(\begin{array}{c|c|c} J_{0,n_1} & & \\ \hline & \ddots & \\ \hline & & J_{0,n_r} \end{array}\right) + \lambda I_{n_1+\ldots+n_r} = \left(\begin{array}{c|c|c} J_{\lambda,n_1} & & \\ \hline & \ddots & \\ \hline & & J_{\lambda,n_r} \end{array}\right) .$$

Unicité : remarquons que :

$$\mathrm{rg}\,(J_{\lambda,n} - \mu I_n)^k = \begin{cases} n & \text{si } \mu \neq \lambda \\ n-k & \text{si } \mu = \lambda \text{ et } 0 \leq k \leq n-1 \\ 0 & \text{si } \mu = \lambda \text{ et } n \leq k \end{cases}$$

donc si la matrice de $u$ dans une certaine base est une matrice de Jordan :

$$\left(\begin{array}{c|c|c} J_{\lambda_1,n_1} & & \\ \hline & \ddots & \\ \hline & & J_{\lambda_r,n_r} \end{array}\right)$$

alors :

$$\mathrm{rg}\,(u - \lambda \mathrm{Id}_E)^k = \sum_{q=1}^{r} \mathrm{rg}\,(J_{\lambda_q,n_q} - \lambda I_{n_q})^k$$

$$= \sum_{\substack{q=1 \\ \lambda_q = \lambda, n_q > k}}^{r} (n_q - k) + \sum_{\substack{q=1 \\ \lambda_q \neq \lambda}}^{r} n_q$$

d'où :

$$\mathrm{rg}\,(u - \lambda \mathrm{Id}_E)^{k-1} - \mathrm{rg}\,(u - \lambda \mathrm{Id}_E)^k = \sum_{\substack{q=1 \\ \lambda_q = \lambda, n_q > k-1}}^{r} ((n_q - (k-1)) - (n_q - k))$$

$$= \sum_{\substack{q=1 \\ \lambda_q = \lambda, n_q \geq k}}^{r} 1$$

et finalement :

$$(\mathrm{rg}\,(u-\lambda\mathrm{Id}_E)^{k-1}-\mathrm{rg}\,(u-\lambda\mathrm{Id}_E)^{k})-(\mathrm{rg}\,(u-\lambda\mathrm{Id}_E)^{k}-\mathrm{rg}\,(u-\lambda\mathrm{Id}_E)^{k+1}) = \sum_{\substack{q=1\\ \lambda_q=\lambda, n_q=k}}^{r} 1$$

$$\Leftrightarrow \mathrm{rg}\,(u-\lambda\mathrm{Id}_E)^{k+1} - 2\mathrm{rg}\,(u-\lambda\mathrm{Id}_E)^{k} + \mathrm{rg}\,(u-\lambda\mathrm{Id}_E)^{k-1} = N_{\lambda,k}\ .$$

<u>*q.e.d.*</u>

**Applications**

— Si $A \in \mathscr{M}_n(\mathbb{C})$, alors $A$ est semblable à ${}^tA$. En effet, il suffit de le vérifier lorsque $A$ est un bloc de Jordan (*exo*) .

— Si $N \in \mathscr{M}_4(\mathbb{K})$ est nilpotente, alors $N$ est semblable à une et une seule des 5 matrices suivantes :

$$0, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} .$$

Il y a une infinité de matrices nilpotentes $4 \times 4$ mais il n'y en a que 5 à similitude près.

— Si $A \in \mathscr{M}_3(\mathbb{K})$ a pour polynôme caractéristique : $\chi_A(X) = (X-1)(X-2)^2$ alors $A$ est semblable

$$\text{à } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \text{ ou à } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} .$$

# Chapitre 7

# Puissances

## 7.1 Motivation

— Problème : résoudre

$$\begin{cases} u_n = au_{n-1} + bv_{n-1} \\ v_n = cv_{n-1} + dv_{n-1} \end{cases}$$

où $a, b, c, d$ sont fixés ou bien :

$$u_n = au_{n-1} + bu_{n-2}$$

où $a, b$ sont fixés.

Ces deux problèmes se réduisent au calcul de $A^k$ où :

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ ou } \begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix} .$$

## 7.2 Cas diagonalisable

— cas diagonal : soient $\lambda_1, ..., \lambda_n \in \mathbb{K}$, alors :

$$^{\forall}k \geq 0, \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}^k = \begin{pmatrix} \lambda_1^k & & \\ & \ddots & \\ & & \lambda_n^k \end{pmatrix} .$$

— cas diagonalisable : si $A = PDP^{-1}$ avec $A, P, D \in \mathscr{M}_n(\mathbb{K})$, $D$ diagonale, $P$ inversible, alors :

$$A^k = PD^kP^{-1} \ .$$

C'est encore plus simple avec les projecteurs spectraux :

$$\text{si } A = \lambda_1\pi_1 + ... + \lambda_r\pi_r$$

où les $\lambda_i$ sont les valeurs propres de $A$ et les $\pi_i$ les projecteurs spectraux associés, alors :

$$^\forall k \geq 0,\ A^k = \lambda_1^k\pi_1 + ... + \lambda_r^k\pi_r$$

c'est vrai aussi pour $k$ entier négatif lorsque tous les $\lambda_i$ sont non nuls. EXEMPLE : Si

$$A := \begin{pmatrix} 1 & \text{—} & 1 \\ | & \diagdown & | \\ 1 & \text{—} & 1 \end{pmatrix} \in \mathscr{M}_n(\mathbb{Q})$$

alors les valeurs propres de $A$ sont 0 et $n$, et :

$$A = n\pi_n \Rightarrow {}^\forall k,\ A^k = n^k\pi_n = n^{k-1}A \ .$$

**Exercice 47** — *Si* $A = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$, *alors :*

$$A = e^{-it}\pi_- + e^{it}\pi_+$$

*où :*

$$\pi_- = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix} \ \textit{et}\ \pi_+ = \frac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix} \ .$$

*Vérifier alors que :*

$$A^k = e^{-ikt}\pi_- + e^{ikt}\pi_+ = \begin{pmatrix} \cos kt & -\sin kt \\ \sin kt & \cos kt \end{pmatrix} \ .$$

— *Si* $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ *alors :*

$$^\forall k \in \mathbb{Z}, A^k = \frac{1}{\sqrt{5}}\begin{pmatrix} \alpha^{k-1} - \alpha'^{k-1} & \alpha^k - \alpha'^k \\ \alpha^k - \alpha'^k & \alpha^{k+1} - \alpha'^{k+1} \end{pmatrix}$$

*où* $\alpha := \frac{1+\sqrt{5}}{2}$ *et* $\alpha' := \frac{1-\sqrt{5}}{2}$.

**Exercice 48** *Soit* $A := \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. *Soit* $\rho$ *l'unique valeur propre réelle de* $A$ *et* $\pi_\rho$ *le projecteur spectral associé.*

*a) Vérifier que* $\pi_\rho = \frac{1}{3\rho^2-1}\begin{pmatrix} \rho^2 & \rho & \rho^3 \\ 1 & \rho^{-1} & \rho \\ \rho & 1 & \rho^2 \end{pmatrix}$.

*b) Vérifier que les deux valeurs propres complexes conjuguées de* $A$ *sont de module* $< 1$ *et en déduire que :*

$$\rho^2 = \lim_{n\infty} \frac{A^n_{1,3}}{A^n_{1,2}}$$

*(cf. page 33)*

***Exercice 49*** *Si* $A := \begin{pmatrix} 1 & 0 & -3 \\ 1 & -1 & -6 \\ -1 & 2 & 5 \end{pmatrix}$, *alors :*

$$\chi_A(X) = m_A(X) = (X-1)(X-2)^2 \ .$$

*Vérifier que :*

$$\pi_1 = \begin{pmatrix} 4 & -6 & -6 \\ 2 & -3 & -3 \\ 0 & 0 & 0 \end{pmatrix} \text{ et } \pi_2 = \begin{pmatrix} -3 & 6 & 6 \\ -2 & 4 & 3 \\ 0 & 0 & 1 \end{pmatrix}$$

*et en déduire que pour tout* $n \geq 0$ *:*

$$A^n = 2^{n-1}\begin{pmatrix} 3n-6 & -6n+12 & -9n+12 \\ 3n-4 & -6n+8 & -9n+6 \\ -n & 2n & 3n+2 \end{pmatrix} + \begin{pmatrix} 4 & -6 & -6 \\ 2 & -3 & -3 \\ 0 & 0 & 0 \end{pmatrix} .$$

## 7.3 Cas général

**Définition 55** *Pour tous entiers $n, k$, on définit le coefficient binomial par :*

$$\binom{n}{k} := C_n^k := \frac{n(n-1)...(n-k+1)}{k!}$$

*si $k \geq n$ et $[\binom{n}{k} := C_n^k := 0$ si $k > n$.*

*Les $\binom{n}{k}$ sont des entiers.*

**Proposition 7.3.1** *Soient $A, B \in \mathscr{M}_n(\mathbb{K})$ deux matrices qui commutent. Alors :*

$$\forall k \geq 0,\ (A+B)^k = \sum_{j=0}^{k} \binom{k}{j} A^j B^{k-j} \quad .$$

En particulier, si $A = D + N$ avec $D$ diagonalisable et $N$ nilpotente qui commutent :

$$A^k = \sum_{j=0}^{k} \binom{k}{j} D^{k-j} N^j \quad .$$

**Proposition 7.3.2** *Soit $A \in \mathscr{M}_n(\mathbb{K})$. On suppose que le polynôme minimal de $A$ est scindé :*

$$m_A(X) = (X - \lambda_1)^{k_1} ... (X - \lambda_r)_r^k$$

*les $\lambda_i$ étant deux à deux distincts. Notons $\pi_1, ..., \pi_r$ les projecteurs spectraux associés aux valeurs propres $\lambda_1, ..., \lambda_r$. Alors :*

$$\forall k \geq 0,\ A^k = \sum_{i=1}^{r} \left( \sum_{j=0}^{\min\{k, k_i - 1\}} \binom{k}{j} \lambda_i^{k-j} (A - \lambda_i I_n)^j \right) \pi_i \quad .$$

*Démonstration :* Il suffit de vérifier cette formule sur chaque sous-espace caractéristique $E^{\lambda_i}$. Or si $x \in E^{\lambda_i}$, $Ax = \lambda_i x + (A - \lambda_i I_n)x$ et $(A - \lambda_i)^{k_i} x = 0$.

*q.e.d.*

## 7.4 Suites récurrentes

**Théorème 7.4.1** *Soient $a_1, ..., a_p \in \mathbb{C}$. On suppose $a_p \neq 0$.*

*On note $P(X) := X^p - a_1 X^{p-1} - ... - a_p$, $\lambda_1, ..., \lambda_r$ ses racines (s.e. distinctes) et $k_1, ..., k_r$ leurs multiplicités respectives.*

*Alors les suites vérifiant :*

$$\forall n \geq p,\ u_n = a_1 u_{n-1} + ... + a_p u_{n-p}$$

*sont les suites de la forme :*

$$u_n = P_1(n)\lambda_1^n + ... + P_r(n)\lambda_r^n$$

*où $P_i$ sont des polynômes de degré $< k_i$.*

— rem : $P_i$ peuvent être déterminés par $u_0, ..., u_{p-1}$.
EXEMPLE : Si $p = 1$,

$$\forall n \geq 1,\ u_n = a_1 u_{n-1} \Leftrightarrow \forall n \geq 1,\ u_n = u_0 a_1^n\ .$$

Si $p = 2$,

$$\forall n \geq 2,\ u_n = a_1 u_{n-1} + a_2 u_{n-2} \Leftrightarrow \forall n \geq 2,\ u_n = \alpha_1 \lambda_1^n + \alpha_2 \lambda_2^n$$

pour certains $\alpha_1, \alpha_2$ si $X^2 - a_1 X - a_2 = (X - \lambda_1)(X - \lambda_2)$ avec $\lambda_1 \neq \lambda_2$ et :

$$\forall n \geq 2,\ u_n = a_1 u_{n-1} + a_2 u_{n-2} \Leftrightarrow \forall n \geq 2,\ u_n = (\alpha n + \beta)\lambda^n$$

pour certains $\alpha, \beta$ si $X^2 - a_1 X - a_2 = (X - \lambda)^2$.

**Exercice 50** *Soit $(u_n)$ la suite définie par :*

$$u_0 = 0,\ u_1 = 1, \forall n \geq 2,\ u_n = u_{n-1} + u_{n-2}$$

*alors :*

$$\forall n \geq 0,\ u_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)\ .$$

*Démonstration* : Si $u_n = n^k \lambda_i^n$, avec $0 \leq k < k_i$, alors pour tout $n \geq p$ :

$$u_n - a_1 u_{n-1} - ... - a_p u_{n-p} = n^k \lambda_i^n - a_1 (n-1)^k \lambda_i^{n-1} - ... - a_p (n-p)^k \lambda_i^{n-p}$$

$$= \lambda_i^{n-p}\left((n-p)^k P(\lambda_i) + (n-p)^{k-1}\lambda_i P'(\lambda_i) + ... + \lambda_i^k P^{(k)}(\lambda_i)\right)$$

$$= 0\ .$$

Réciproquement, si :

$$\forall n \geq p,\ u_n = a_1 u_{n-1} + ... + a_p u_{n-p}$$

alors on pose :

$$X_n := \begin{pmatrix} u_{n-p+1} \\ \vdots \\ u_n \end{pmatrix} \in \mathbb{K}^p \ .$$

On a alors :

$$\forall n \geq p,\ X_n = AX_{n-1}$$

où $A \in \mathscr{M}_p(\mathbb{K})$ est la transposée de la matrice compagnon du polynôme $P(X)$ :

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ & & & & 0 \\ 0 & \cdots & & 0 & 1 \\ a_p & \cdots & & & a_1 \end{pmatrix}$$

donc :

$$\chi_A(X) = (X - \lambda_1)^{k_1}...(X - \lambda_r)^{k_r} \ .$$

Notons $\pi_1, ...\pi_r$ les projecteurs spectraux correspondants. D'après la proposition 7.3.2,

$$\forall n \geq p,\ A^n = \sum_{i=1}^{r} \left( \sum_{j=0}^{\min\{n,k_i-1\}} \binom{n}{j} \lambda_i^{n-j} (A - \lambda_i I_n)^j \right) \pi_i$$

$$= \sum_{i=1}^{r} \lambda_i^n \left( \sum_{j=0}^{k_i-1} \frac{\binom{n}{j}}{\lambda_i^j} (A - \lambda_i I_n)^j \right) \pi_i \ .$$

Or,

$$\forall n \geq p,\ X_n = A^{n-p+1} X_{p-1}$$
$$= A^n X_0$$

si on pose $X_0 := A^{1-p} X_{p-1}$.

Donc, $u_n$ est la dernière composante du vecteur :

$$\sum_{i=1}^{r} \lambda_i^n \sum_{j=0}^{k_i-1} \binom{n}{j} \frac{(A - \lambda_i I_n)^j \pi_i(X_0)}{\lambda_i^j}$$

et il suffit de remarquer que si $0 \leq j \leq k_i - 1$,

$$\binom{n}{j} = \frac{n(n-1)...(n-j+1)}{j!}$$

est un polynôme en $n$ de degré $< k_i$. <u>*q.e.d.*</u>

# Chapitre 8

# Exponentielle

Dans ce chapitre, les matrices sont complexes !
Motivation : système différentiel linéaire + formule de Taylor

## 8.1 Exponentielle complexe

Rappelons que :

— toute série numérique $\sum_{k=0}^{\infty} a_k$ à termes réels positifs (ou nuls) converge (dans $\mathbb{R}$) si et seulement si la suite de ses sommes partielles $\sum_{k=0}^{N} a_k$ est bornée.

— toute série de nombres complexes $\sum_{k=0}^{\infty} z_k$ absolument convergente converge

$$\textit{c-à-d} \ : \sum_{k=0}^{\infty} |z_k| < \infty \Rightarrow \sum_{k=0}^{\infty} z_k \text{ converge dans } \mathbb{C}.$$

— Pour tout nombre complexe :

$$\exp z := e^z := \sum_{k=0}^{\infty} \frac{z^k}{k!}$$

et :

$$e^0 = 1, e^{z+z'} = e^z e^{z'} \ (^\forall z, z' \in \mathbb{C}) \ .$$

## 8.2 Suites de matrices

**Définition 56** *On dit qu'une suite $(A_k)_{k\in\mathbb{N}}$ de matrices complexes converge vers une matrice $A$ si pour tous $i, j$ la suite des coefficients $A_{k,i,j}$ converge vers le coefficient $A_{i,j}$ dans $\mathbb{C}$.*

On pose :

$$|||A||| := \max_i \sum_j |a_{i,j}|$$

pour toute matrice $A$.

— propriétés : c'est une norme multiplicative ! *c-à-d* : pour toutes matrices $A, B \in \mathscr{M}_n(\mathbb{C})$, pour tout $\lambda \in \mathbb{C}$, on a :

i) $|||A||| = 0 \Leftrightarrow A = 0$ ;

ii) $|||A + B||| \leq |||A||| + |||B|||$ ;

iii) $|||\lambda A||| = |\lambda||||A|||$ ;

iv) $|||AB||| \leq |||A||||||B|||$.

**Remarque :** Si $A = (a_{i,j})_{1 \leq i,j \leq n}$, alors pour tous $i, j$, $|a_{i,j}| \leq |||A|||$. On en déduit qu'une suite de matrices $(A_k)_{k \in \mathbb{N}}$ converge vers une matrice $A$ si :

$$\lim_{k \to \infty} |||A_k - A||| = 0 \ .$$

**Exercice 51** *En déduire que si* $(A_k)$ *et* $(B_k)$ *sont des suites de matrices qui convergent vers* $A$ *et* $B$*, alors :*

$$\lim_{k \to \infty} A_k B_k = AB \ .$$

**Exercice 52** *On pose pour tout* $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$ *:* $||X|| := \max_{i=1}^n |x_i|$.

*Alors :*

$$|||A||| = \max_{\substack{X \in \mathbb{K}^n \\ X \neq 0}} \frac{||AX||}{||X||}$$

*pour toute matrice* $A \in \mathscr{M}_n(\mathbb{C})$.

## 8.3 Définition de $\exp(A)$

**Théorème 8.3.1** *Pour toute matrice* $A \in \mathscr{M}_n(\mathbb{C})$*, la série :*

$$\sum_{k=0}^{\infty} \frac{A^k}{k!}$$

*converge dans* $\mathscr{M}_n(\mathbb{C})$*. On note :*

$$\exp A := e^A := \sum_{k=0}^{\infty} \frac{A^k}{k!}$$

*sa limite. C'est la matrice exponentielle de* $A$*.*

*Démonstration :* Il suffit de démontrer que les séries de coefficients convergent. Or pour tous $i, j$, on a :

$$\sum_{k=0}^{\infty} \left| \frac{A^k_{i,j}}{k!} \right| \leq \sum_{k=0}^{\infty} \left| \frac{|||A^k|||}{k!} \right|$$

$$\leq \sum_{k=0}^{\infty} \frac{|||A|||^k}{k!}$$

$$= e^{|||A|||} < \infty \ .$$

Donc pour tous $i, j$, la série $\sum_{k=0}^{\infty} \frac{A^k_{i,j}}{k!}$ converge dans $\mathbb{C}$. q.e.d.

**Exercice 53** *Pour une matrice diagonale* $D := \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$*, on a*

$$\exp D = \begin{pmatrix} e^{\lambda_1} & & \\ & \ddots & \\ & & e^{\lambda_n} \end{pmatrix} \ .$$

**Théorème 8.3.2 (propriétés de l'exponentielle)** *On a :*

$$\exp 0 = I_n \text{ et } \exp(A+B) = \exp A \exp B$$

*pour toutes matrices $A$ et $B$ qui commutent. En particulier, pour tout $A \in \mathscr{M}_n(\mathbb{C})$, la matrice* $\exp A$ *est inversible d'inverse* $\exp(-A)$*. On a aussi :*

$$\exp(kA) = (\exp A)^k$$

*pour tout $k \in \mathbb{Z}$.*

**Remarque :** Attention ! si $A, B$ ne commutent pas, en général $\exp(A+B) \neq \exp A \exp B$.

**Remarque :** En fait l'application : $\exp : \mathscr{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ est surjective.

*Démonstration :* Montrons que $\exp(A+B) = \exp A \exp B$ :

$$\forall m \geq 0 \ : \left( \sum_{i=0}^{m} \frac{A^i}{i!} \right) \left( \sum_{j=0}^{m} \frac{B^j}{j!} \right) - \sum_{k=0}^{m} \frac{(A+B)^k}{k!}$$

$$= \sum_{0\leq i,j\leq m} \frac{A^i}{i!}\frac{B^j}{j!} - \sum_{k=0}^{m} \sum_{\substack{i,j\geq 0\\ i+j=k}} \frac{A^i}{i!}\frac{B^j}{j!}$$

$$= \sum_{0\leq i,j\leq m} \frac{A^i}{i!}\frac{B^j}{j!} - \sum_{\substack{0\leq i,j\leq m\\ i+j\leq m}} \frac{A^i}{i!}\frac{B^j}{j!}$$

$$= \sum_{\substack{0\leq i,j\leq m\\ i+j> m}} \frac{A^i}{i!}\frac{B^j}{j!}$$

donc :

$$\forall m \geq 0,\ |||\left(\sum_{i=0}^{m} \frac{A^i}{i!}\right)\left(\sum_{j=0}^{m} \frac{B^j}{j!}\right) - \sum_{k=0}^{m} \frac{(A+B)^k}{k!}|||$$

$$\leq ||| \sum_{\substack{0\leq i,j\leq m\\ i+j> m}} \frac{A^i}{i!}\frac{B^j}{j!}|||$$

$$\leq \sum_{\substack{0\leq i,j\leq m\\ i+j> m}} |||\frac{A^i}{i!}\frac{B^j}{j!}|||$$

$$\leq \sum_{\substack{0\leq i,j\leq m\\ i+j> m}} \frac{|||A|||^i}{i!}\frac{|||B|||^j}{j!}$$

$$\leq \left(\sum_{i=0}^{m} \frac{|||A|||^i}{i!}\right)\left(\sum_{j=0}^{m} \frac{|||B|||^j}{j!}\right) - \sum_{k=0}^{m} \frac{(|||A|||+|||B|||)^k}{k!}$$

et si « on fait tendre $m$ vers $+\infty$ » on trouve :

$$|||\exp A \exp B - \exp(A+B)||| \leq e^{|||A|||}e^{|||B|||} - e^{|||A|||+|||B|||} = 0$$

donc : $\exp A \exp B = \exp(A+B)$. <u>*q.e.d.*</u>

**Exercice 54** *Vérifier que :*

$$\exp\left(t.\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right) = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$$

*pour tout $t$ réel.*

## 8.4 Méthode de calcul

**Exercice 55** *Si* $P \in \mathrm{GL}_n(\mathbb{C}), D \in \mathscr{M}_n(\mathbb{C})$ *(par exemple* $D$ *diagonale), alors :*

$$\exp(PDP^{-1}) = P \exp D P^{-1} \ .$$

*En déduire que pour toute matrice* $A \in \mathscr{M}_n(\mathbb{C})$*,*

$$\text{dét} \exp A = e^{\mathrm{tr} A} \ .$$

**Proposition 8.4.1** *Soit* $A \in \mathscr{M}_n(\mathbb{C})$*. Soit*

$$m_A(X) = (X - \lambda_1)^{k_1} ... (X - \lambda_r)^{k_r}$$

*le polynôme minimal de* $A$*, les* $\lambda_i$ *étant les valeurs propres deux à deux distinctes de* $A$*. Notons* $\pi_1, ... \pi_r$ *les projecteurs spectraux associés aux* $\lambda_i$*.*

*Alors :*

$$\exp(tA) = \sum_{i=1}^{r} e^{t\lambda_i} \left( \sum_{j=0}^{k_i - 1} t^j \frac{(A - \lambda_i I_n)^j}{j!} \right) \pi_i \ .$$

*En particulier,* $\exp A$ *est un polynôme en* $A$*.*

**Remarque :** Si $A$ est diagonalisable, alors, pour tout $t \in \mathbb{C}$, $\exp(tA) = e^{t\lambda_1}\pi_1 + ... + e^{t\lambda_r}\pi_r$.

*Démonstration :* On décompose $A$ en :

$$A = D + N$$

avec $D$ diagonalisable et $N$ nilpotente qui commutent. Alors :

$$\exp A = \exp D \exp N \ .$$

Or,

$$D = \sum_{i=1}^{r} \lambda_i \pi_i \Rightarrow \forall k \geq 0, \ \frac{D^k}{k!} = \sum_{i=1}^{r} \frac{\lambda_i^k}{k!} \pi_i$$

et on en déduit que :

$$\exp D = \sum_{k=0}^{\infty} \frac{D^k}{k!} = \sum_{i=1}^{r} \left( \sum_{k=0}^{\infty} \frac{\lambda_i^k}{k!} \right) \pi_i$$

$$= \sum_{i=1}^{r} e^{\lambda_i} \pi_i \ .$$

D'un autre côté, on a :

$$\begin{aligned} N &= \sum_{i=1}^{r} N\pi_i \\ &= \sum_{i=1}^{r} (A - \lambda_i I_n)\pi_i \\ \Rightarrow \forall k \geq 0 \, N^k &= \sum_{i=1}^{r} (A - \lambda_i I_n)^k \pi_i \end{aligned}$$

or : $\forall k \geq k_i$, $(A - \lambda_i I_n)^k \pi_i = 0$ (*exo*) .

Donc :

$$\begin{aligned} \exp N &= \sum_{k=0}^{\infty} \frac{N^k}{k!} \\ &= \sum_{i=1}^{r} \sum_{k=0}^{k_i - 1} \frac{(A - \lambda_i I_n)^k}{k!} \pi_i \ . \end{aligned}$$

*q.e.d.*

Exemple : Si

$$A := \begin{pmatrix} 1 & 0 & -3 \\ 1 & -1 & -6 \\ -1 & 2 & 5 \end{pmatrix}$$

alors

$$\begin{aligned} \exp(tA) &= e^{2t}(I_3 + t(A - 2I_3))\pi_2 + e^t \pi_1 \\ &= e^{2t} \begin{pmatrix} 3t-3 & -6t+6 & -9t+6 \\ 3t-2 & -6t+4 & -9t+3 \\ -t & 2t & 3t+1 \end{pmatrix} + e^t \begin{pmatrix} 4 & -6 & -6 \\ 2 & -3 & -3 \\ 0 & 0 & 0 \end{pmatrix} \ . \end{aligned}$$

## 8.5 Équations différentielles

### 8.5.1 Dérivation des matrices

On dit qu'une fonction $f$ définie sur un intervalle ouvert $I$ de $\mathbb{R}$ et à valeurs dans $\mathbb{C}$ est dérivable en $t_0 \in I$ si la limite :

$$\lim_{\substack{t \to t_0 \\ t \neq t_0}} \frac{f(t) - f(t_0)}{t - t_0}$$

existe dans $\mathbb{C}$. On dit que $f$ est dérivable sur $I$ si elle l'est en tout $t_0 \in I$.

**Définition 57** *Soient $a_{i,j} : I \to \mathbb{C}$, $i, j$, des fonctions dérivables sur un intervalle $I$ de $\mathbb{R}$. On dit que la matrice $A(t) := (a_{i,j}(t))_{1\le i\le p, 1\le j\le q}$ est dérivable et on note $A'(t) := (a'_{i,j}(t))_{1\le i\le p,1\le j\le q}$.*

**Exercice 56** *Vérifier que si pour tout $t \in I$, $A(t) \in \mathscr{M}_{p,q}(\mathbb{C})$ et $B(t) \in \mathscr{M}_{q,r}(\mathbb{C})$ et si les matrices $A$ et $B$ sont dérivables sur $I$, alors le produit aussi et on a :*

$$\forall t \in I,\ (AB)'(t) = A'(t)B(t) + A(t)B'(t)\ .$$

**Proposition 8.5.1** *Soit $A \in \mathscr{M}_n(\mathbb{C})$. La matrice :*

$$t \mapsto \exp(tA)$$

*est dérivable sur $\mathbb{R}$ et on a :*

$$\forall t\ \in \mathbb{R},\ (\exp(tA))' = A\exp(tA) = \exp(tA)A\ .$$

*Démonstration* : Soient $\pi_1, ..., \pi_r$ les projecteurs spectraux de $A$. Alors d'après la proposition 8.4.1, on a :

$$\exp(tA) = \sum_{i=1}^{r}\sum_{k=0}^{\infty} e^{t\lambda_i}\frac{t^k}{k!}(A-\lambda_i)^k\pi_i$$

(la somme sur $k$ est en fait finie car $(A - \lambda_i I_n)^k\pi_i = 0$ pour $k$ assez grand). Donc :

$$t \mapsto \exp(tA)$$

et dérivable de dérivée :

$$(\exp(tA))' = \sum_{i=1}^{r}\sum_{k=0}^{\infty} e^{t\lambda_i}(\lambda_i\frac{t^k}{k!} + k\frac{t^{k-1}}{k!})(A-\lambda_i I_n)^k\pi_i$$

$$= \sum_{i=1}^{r}\sum_{k=0}^{\infty} e^{t\lambda_i}\lambda_i\frac{t^k}{k!}(A-\lambda_i I_n)^k\pi_i + \sum_{i=1}^{r}\sum_{k=0}^{\infty} e^{t\lambda_i}\frac{t^k}{k!}(A-\lambda_i I_n)^{k+1}\pi_i$$

$$= \sum_{i=1}^{r}\sum_{k=0}^{\infty} e^{t\lambda_i}\frac{t^k}{k!}(\lambda_i I_n + (A-\lambda_i I_n))(A-\lambda_i I_n)^k\pi_i$$

$$= A\exp(tA)\ .$$

*q.e.d.*

### 8.5.2 Équations différentielles linéaires à coefficients constants

Ce sont les équations de la forme :

$$Y'(t) = AY(t)$$

où $A \in \mathscr{M}_n(\mathbb{C})$ est une matrice **constante** et $Y(t) = \begin{pmatrix} y_1(t) \\ \vdots \\ y_n(t) \end{pmatrix}$ est un vecteur inconnu dont les coordonnées sont des fonctions dérivables.

— cas homogène :

**Théorème 8.5.2**

$$Y' = AY \Leftrightarrow Y(t) = \exp(tA)Y(0)$$

*en particulier les solutions sont définies sur* $\mathbb{R}$ *tout entier.*

*Démonstration :* D'un côté, le membre de doite est bien solution de l'équation $Y' = AY$ (*exo*) . Réciproquement, si on pose $Z(t) := \exp(-tA)Y(t)$, alors :



$$Z'(t) = \exp(-tA)(Y' - AY) = 0$$

Donc sur $\mathbb{R}$, $Z$ est constante et $Z(t) = Z(0) = Y(0)$ pour tout $t$. *q.e.d.*

Exemple : Le système :

$$\begin{cases} x_1'(t) &= x_1(t) - 3x_3(t) \\ x_2'(t) &= x_1(t) - x_2(t) - 6x_3(t) \\ x_3'(t) &= -x_1(t) + 2x_2(t) + 5x_3(t) \end{cases}$$

avec pour « conditions initiales » $x_1(0) = 1, x_2(0) = 1, x_3(0) = 0$ a pour solution :

$$\begin{pmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \end{pmatrix} = \exp(tA) \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

où $A$ est la matrice $\begin{pmatrix} 1 & 0 & -3 \\ 1 & -1 & -6 \\ -1 & 2 & 5 \end{pmatrix}$. On trouve alors :

$$\begin{aligned} x_1(t) &= (-3t+3)e^{2t} - 2e^t\,, \\ x_2(t) &= (-3t+2)e^{2t} - e^t\,, \\ x_3(t) &= te^{2t}\ . \end{aligned}$$

— solutions de l'équation différentielle linéaire d'ordre $p$ à coefficients constants.

**Corollaire 8.5.2.1** *Soient $a_1, ..., a_p \in \mathbb{C}$ tels que $a_p \neq 0$. On suppose que :*

$$\chi(X) := X^p + a_1 X^{p-1} + ... + a_p = (X - \lambda_1)^{m_1} ... (X - \lambda_r)^{m_r}$$

*pour certains $\lambda_i \in \mathbb{C}$ deux à deux distincts et certains entiers $m_i \geq 1$.*

*Alors :*

$$(E)\ y^{(p)} + a_1 y^{(p-1)} + ... + a_p y = 0 \Leftrightarrow {}^\forall t \in \mathbb{R},\ y(t) = \sum_{i=1}^{r} e^{\lambda_i t} P_i(t)$$

*pour certains polynômes $P_i$ de degré $< m_i$ (pour tout $i$).*

**Remarque :** On peut déterminer les $P_i$ en fonction des valeurs $y(0), ..., y^{(p-1)}(0)$.

*Démonstration* : **⇒ :** On pose $Y(t) := \begin{pmatrix} y(t) \\ y'(t) \\ \vdots \\ y^{(p-1)}(t) \end{pmatrix} \in \mathbb{C}^p$ pour tout $t$.

Alors :

$$(E) \Leftrightarrow Y'(t) = AY(t)$$

où $A$ est la matrice

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ -a_p & \cdots & \cdots & \cdots & -a_1 \end{pmatrix}.$$

Remarquons que $\chi(X) = \chi_A(X) = m_A(X)$.

On a donc

$$Y(t) = \exp(tA)Y(0)$$

avec :

$$\exp(tA) := \sum_{i=1}^{r} e^{t\lambda_i} \left( \sum_{k=0}^{m_i-1} \frac{t^k}{k!}(A - \lambda_i I_p)^k \right) \pi_i$$

où les $\pi_i$ sont les projecteurs spectraux associés aux $\lambda_i$.

Or $y(t)$ est le premier coefficient de $Y(t)$ donc :

$$y(t) = \sum_{i=1}^{r} e^{\lambda_i t} \underbrace{\sum_{k=0}^{m_i-1} \frac{t^k}{k!} \Big( (A - \lambda_i I_n)^k \pi_i(Y(0)) \Big)_1}_{=:P_i(t)} \ .$$

**⇐:** Il suffit de vérifier que $y : t \mapsto e^{\lambda_i t} P_i(t)$ est solution de $(E)$ pour tout polynôme de degré $< m_i$. Or pour une telle fonction $y$, on a (en posant $a_0 := 1$) :

$$^{\forall} t \in \mathbb{R},\ y^{(p)}(t) + a_1 y^{(p-1)}(t) + ... + a_p y(t) = \sum_{k=0}^{p} a_k \sum_{j=0}^{k} \binom{k}{j} \lambda_i^{k-j} e^{\lambda_i t} P_i^{(j)}(t)$$

$$= \sum_{\substack{j=0 \\ j<m_i}}^{p} e^{\lambda_i t} P_i^{(j)}(t) \underbrace{\sum_{k=j}^{p} a_k \frac{k!}{(k-j)!} \lambda_i^{k-j}}_{=\chi^{(j)}(\lambda_i)=0}$$

$$= 0 \ .$$

<u>*q.e.d.*</u>

# Chapitre 9

# Groupe orthogonal

## 9.1 Matrices orthogonales

**Définition 58** *Une matrice $A$ est orthogonale si ${}^tAA = I_n$.*

Exemple :

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \text{ et } \frac{1}{3}\begin{pmatrix} 2 & -2 & 1 \\ 1 & 2 & 2 \\ 2 & 1 & -2 \end{pmatrix}$$

sont orthogonales.

**Remarque :** $A$ orthogonale $\Leftrightarrow$ $A$ inversible et $A^{-1} = {}^tA \Leftrightarrow A{}^tA = I_n$.

**Remarque :** Si $A$ est orthogonale, alors $(\text{dét}\, A)^2 = \text{dét}\,({}^tAA) = 1$ donc $\text{dét}\, A = \pm 1$.

**Définition 59** *On note $O_n(\mathbb{R})$ l'ensemble des matrices $n \times n$ réelles orthogonales et $SO_n(\mathbb{R})$ l'ensemble des matrices $n \times n$ réelles orthogonales de déterminant 1. Les éléments de $SO_n(\mathbb{R})$ sont les rotations de $\mathbb{R}^n$.*

**Remarque :** $I_n \in O_n(\mathbb{R})$, $\forall A \in O_n(\mathbb{R})$, $A^{-1} \in O_n(\mathbb{R})$ $\forall A, B \in O_n(\mathbb{R})$, $AB \in O_n(\mathbb{R})$ donc $O_n(\mathbb{R})$ est un sous-groupe de $GL_n(\mathbb{R})$. De même $SO_n(\mathbb{R})$ est un sous-groupe de $GL_n(\mathbb{R})$.

## 9.2 Produit scalaire

**Définition 60** *Le produit scalaire standard sur $\mathbb{R}^n$ est l'application :*

$$\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R} \ \ (X, Y) \mapsto {}^tXY$$

*(si* $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ *et* $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$, *alors* $\langle X, Y\rangle = x_1y_1 + ... + x_ny_n$*).*

*Propriétés :*

$$\forall x, y, z \in \mathbb{R}^n,\ \langle x, y+z\rangle = \langle x, y\rangle + \langle x, z\rangle$$

$$\forall x, y, z \in \mathbb{R}^n,\ \langle x+y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$$

$$\forall x, y \in \mathbb{R}^n,\ \forall t \in \mathbb{R},\ \langle x, ty\rangle = \langle tx, y\rangle = t\langle x, y\rangle$$

$$\forall x, y \in \mathbb{R}^n,\ \langle x, y\rangle = \langle y, x\rangle$$

$$\forall x \in \mathbb{R}^n,\ \langle x, x\rangle \geq 0 \text{ et } \langle x, x\rangle = 0 \Leftrightarrow x = 0\ .$$

**Définition 61** *On pose pour tout* $x \in \mathbb{R}^n$, $||x|| = \sqrt{\langle x, x\rangle}$.

*Nouvelle caractérisation de la transposée*

**Proposition 9.2.1** *Pour tous* $X, Y \in \mathbb{R}^n$*, pour toute matrice réelle* $A \in \mathscr{M}_n(\mathbb{R})$*, on :*

$$\langle AX, Y\rangle = \langle X, {}^tAY\rangle\ .$$

*Démonstration :* Évident ! *q.e.d.*

**Proposition 9.2.2** *Soit* $A \in \mathscr{M}_n(\mathbb{R})$*. Alors sont équivalentes :*
*i) A est orthogonale ;*
*ii)* $\forall X \in \mathbb{R}^n$ , $||AX|| = ||X||$ *;*
*iii)* $\forall X, Y \in \mathbb{R}^n$, $\langle AX, AY\rangle = \langle X, Y\rangle$.

*Démonstration :* ***i) ⇒ ii)*** : Si $A$ est orthogonale et si $X \in \mathbb{R}^n$, alors :

$$||AX||^2 = \langle AX, AX\rangle = \langle X, {}^tAAX\rangle = \langle X, X\rangle\ .$$

***ii) ⇒ iii)*** : si $\forall X \in \mathbb{R}^n$ , $||AX|| = ||X||$, alors pour tout $X, Y \in \mathbb{R}^n$ :

$$||A(X+Y)||^2 = ||X+Y||^2$$

$$\Leftrightarrow \langle AX + AY, AX + AY\rangle = \langle X+Y, X+Y\rangle$$

$$\Leftrightarrow \langle AX, AX\rangle + 2\langle AX, AY\rangle + \langle AY, AY\rangle = \langle X, X\rangle + 2\langle X, Y\rangle + \langle Y, Y\rangle$$

$$\Leftrightarrow \langle AX, AY\rangle = \langle X, Y\rangle \ .$$

***iii)*** $\Rightarrow$ ***i)*** :

On a :

$$\forall X, Y \in \mathbb{R}^n,\ \langle AX, AY\rangle = \langle X, Y\rangle$$
$$\Leftrightarrow \forall X, Y \in \mathbb{R}^n,\ \langle {}^tAAX, Y\rangle = \langle X, Y\rangle$$
$$\Leftrightarrow \forall X, Y \in \mathbb{R}^n,\ \langle {}^tAAX - X, Y\rangle = 0$$

en particulier si $Y = {}^tAAX - X$, on trouve :

$$||{}^tAAX - X||^2$$

donc ${}^tAAX = X$ pour tout $X \in \mathbb{R}^n$ d'où ${}^tAA = I_n$.

*q.e.d.*

## 9.3 Réflexions orthogonales

**Définition 62** *Une réflexion orthogonale est une matrice $R \in \mathscr{M}_n(\mathbb{R})$ telle que :*

$$i) R = {}^tR\,,\ ii) R^2 = I_n,\ ,iii) \dim\ker(R - I_n) = n - 1\ .$$

En particulier, les réflexions orthogonales sont des matrices orthogonales.

Exemple : $R = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

**Définition 63** *Soit $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{R}^n$ tel que $||v|| = 1$. On définit :*

$$G(v_1, ..., v_n) := \begin{pmatrix} v_i v_j \end{pmatrix}_{1 \le i,j \le n} \in \mathscr{M}_n(\mathbb{R})$$

*et :*

$$R_v := I_n - 2G(v_1, ..., v_n)\ .$$

**Proposition 9.3.1** *La matrice $R_v$ est une réflexion orthogonale et :*

$$\forall X \in \mathbb{R}^n,\ R_v(X) = X - 2\langle v, X\rangle v\ .$$

*Démonstration :* Si $G = [G(v_1, ..., v_n)$ avec $v_1, ..., v_n \in \mathbb{R}$ tels que $v_1^+ ... + v_n^2 = 1$, alors : $G^2 = G$ et ${}^tG = G$. Donc $R_v$ est orthogonale car ${}^tR_v = R_v$, $R_v^2 = I_n - 4G + 4G^2 = I_n$ et $R_v - I_n = -2G$ qui est une matrice de rang 1 donc de noyau de dimension $n - 1$.

De plus, si $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ et si $R_v(X) = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$, alors :

$$y_i = x_i - 2\sum_{j=1}^{n} v_i v_j x_j = x_i - 2\langle v, X\rangle v_i$$

pour tout $1 \leq i \leq n$ d'où : $R_v - X) = X - 2\langle v, X\rangle v$.

<u>*q.e.d.*</u>

**Lemme 9.3.2** *Soient $x, x' \in \mathbb{R}^n$ tels que $||x|| = ||x'|| = 1$. Alors il existe $R \in O_n(\mathbb{R})$ tel que $Rx = x'$.*

*Démonstration :* Si $x \neq x'$, il suffit de prendre $R = R_v$ où $v := \frac{x-x'}{||x-x'||}$.

<u>*q.e.d.*</u>

# 9.4 Réduction des matrices orthogonales

## 9.4.1 $O_2(\mathbb{R})$

Soit $\theta \in \mathbb{R}$. On notera $\Delta_\theta := \mathbb{R}\begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$ la droite du plan $\mathbb{R}^2$ passant par 0 et qui fait un angle $\theta$ avec « l'axe des abscisses » .

**Exercice 57** *Vérifier que les matrices*

$$\rho_t := \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix} \text{ et } R_t := \begin{pmatrix} \cos t & \sin t \\ \sin t & -\cos t \end{pmatrix}$$

*sont orthogonales. Ce sont respectivement la matrice de la rotation (de centre 0) et d'angle $t$ et la matrice de la réflexion orthogonale par rapport à l'axe $\Delta_{\frac{t}{2}}$. Remarquer que* $\text{dét}\, \rho_t = -\text{dét}\, R_t = 1$.

Nous allons voir que ce sont les seules matrices orthogonales $2 \times 2$.

**Proposition 9.4.1**

$$O_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix} \; : \; t \in \mathbb{R} \right\} \cup \left\{ \begin{pmatrix} \cos t & \sin t \\ \sin t & -\cos t \end{pmatrix} \; : \; t \in \mathbb{R} \right\}$$

$$SO_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix} \; : \; t \in \mathbb{R} \right\} \; .$$

*Démonstration :*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O_2(\mathbb{R}) \Leftrightarrow \begin{cases} a^2 + c^2 = 1 \\ ab + cd = 0 \\ b^2 + d^2 = 1 \end{cases}$$

donc il existe $\theta \in \mathbb{R}$ tel que $a = \cos\theta$, $c = \sin\theta$. De plus $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc :$ $\epsilon = \pm 1$.

On a donc :

$$\begin{cases} \cos\theta d - \sin\theta b = \epsilon \\ \sin\theta d + \cos\theta b = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} d = \epsilon \cos\theta \\ b = -\epsilon \sin\theta \end{cases} \; .$$

*q.e.d.*

**Exercice 58**

$$^{\forall} t, t' \in \mathbb{R}, \; \rho_t \rho_{t'} = \rho_{t+t'} \; , \; R_{t'} R_t = \rho_{2(t'-t)}$$

**Exercice 59** *En déduire que $O_2(\mathbb{R})$ est engendré par les réflexions orthogonales.*

**Exercice 60** *On a un isomorphisme de groupes :*

$$S^1 \to SO_2(\mathbb{R})$$

$$e^{it} \mapsto \rho_t$$

*en particulier,* $SO_2(\mathbb{R})$ *est commutatif !*

**Remarque :** Pour une rotation $r \in SO_2(\mathbb{R})$, $r = \rho_t \Rightarrow \mathrm{tr} r = 2\cos t$.

**Exercice 61** *Pour tout* $t$, $R_t = \rho_{\frac{t}{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \rho_{-\frac{t}{2}}$.

### 9.4.2 $O_3(\mathbb{R})$

**Théorème 9.4.2** *Soit* $A \in O_3(\mathbb{R})$. *Il existe* $\epsilon = \pm 1$, $t \in \mathbb{R}$ *et* $P \in O_3(\mathbb{R})$ *tels que :*

$$A = P \begin{pmatrix} \epsilon & 0 & 0 \\ 0 & \cos t & -sint \\ 0 & \sin t & \cos t \end{pmatrix} P^{-1}$$

*(remarque : alors* $\epsilon = \mathrm{dét}\, A$ *et* $\cos\theta = \frac{\mathrm{tr} A - 1}{2}$*).*

*Démonstration :* Supposons que $\mathrm{dét}\, A = 1$. Comme le polynôme caractéristique de $A$ est réell de degré 3, il admet 3racines réelles $\lambda_1, \lambda_2, \lambda_3$ ou une racine réelle $\lambda$ et deux racines complexes conjuguées $\mu, \overline{\mu}$. Dans le prmier cas $\lambda_1\lambda_2\lambda_3 = 1$ et dans le second : $\lambda|\mu|^2 = 1$. Dans les deux cas, $A$ admet au moins une valeur propre réelle $\lambda > 0$. Il existe alors $v \in \mathbb{R}^3$ de norme 1 tel que : $Av = \lambda v$.Comme $||Av|| = ||v||$, on a :

$$||\lambda v|| = \lambda = 1$$

donc 1 est valeur propre de $A$.

Il existe $P \in O_3(\mathbb{R})$ tel que $P \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = v$. Mais alors :

$$Av = v$$

$$\Leftrightarrow AP \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = P \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$P^{-1}AP \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} .$$

Posons $B := P^{-1}AP$. La matrice $B$ est orthogonale car $P$ et $A$ le sont et comme

$$B \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} ,$$

$B$ est de la forme :

$$\begin{pmatrix} 1 & \alpha & \beta \\ 0 & a & b \\ 0 & c & d \end{pmatrix} .$$

Donc : ${}^tBB = I_3 \Rightarrow \alpha = \beta = 0$ et $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SO_2(\mathbb{R})$ (car $\text{dét}\, B = 1$).

Or, on a déjà vu que :

$$SO_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix} \; : \; t \in \mathbb{R} \right\} .$$

Si $\text{dét}\, A = -1$, on est ramené au cas précédent avec $-A$ à la place de $A$.

*q.e.d.*

**Définition 64** *Soit $I_3 \neq A \in SO_3(\mathbb{R})$. On appelle axe de la rotation $A$ la droite :* $\ker(A - I_3)$ *(c'est bien une droite (exo) ).*

**Exercice 62** *Soient $t, t' \in \mathbb{R}$. S'il existe $P \in O_3(\mathbb{R})$ tel que :*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos t & -sint \\ 0 & \sin t & \cos t \end{pmatrix} = P \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos t' & -sint' \\ 0 & \sin t' & \cos t' \end{pmatrix} P^{-1}$$

*alors $t = \pm t' \mod 2\pi$ (indication : calculer la trace ).*

*« Réciproquement » :*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos t & -sint \\ 0 & \sin t & \cos t \end{pmatrix} = P \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(-t) & -sin(-t) \\ 0 & \sin(-t) & \cos(-t) \end{pmatrix} P^{-1}$$

*avec* $P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.

### 9.4.3 Cas général

**Théorème 9.4.3** *Soit $A \in O_n(\mathbb{R})$. Alors il existe une matrice orthogonale $P$ telle que :*

$$A = PRP^{-1}$$

*où $R$ est de la forme :*

$$R = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & -1 & & & \\ & & & & \ddots & & \\ & & & & & -1 & \\ & & & & & & \rho_{\theta_1} \\ & & & & & & & \ddots \\ & & & & & & & & \rho_{\theta_r} \end{pmatrix}$$

*où* $\rho_{\theta_i} = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix}$.

**Remarque :** Si le nombre de $-1$ dans la matrice réduite est impair, $\text{dét}\, A = -1$, $\text{dét}\, A = 1$ sinon.

*Cas où $n = 2, 3$ :* Si $n = 2$, $A = \rho_\theta$ ou $A = P \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} P^{-1}$ pour une certaine matrice orthogonale $P$.

Si $n = 3$, alors :

$$A = P \begin{pmatrix} \epsilon & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} P^{-1}$$

pour une certaine matrice orthogonale $P$ et $\epsilon = \pm 1$.

*Démonstration :* On raisonne par récurrence sur $n$. Notons $e_1, ..., e_n$ la base canonique de $\mathbb{R}^n$. Soit $A \in O_n(\mathbb{R})$. Soit $\lambda \in \mathbb{C}$ une valeur propre de $A$. Si $\lambda \in \mathbb{R}$, alors $\lambda = \pm 1$. Soit $v$ un vecteur propre de norme 1 associé. Soit $P \in O_n(\mathbb{R})$ tel que $Pe_1 = v$. Alors :

$$P^{-1}APe_1 = e_1$$

donc $P^{-1}AP$ est orthogonale de la forme :

$$\begin{pmatrix} 1 & 0 & ... & 0 \\ 0 & b_{1,1} & ... & \\ \vdots & ... & & \\ 0 & ... & & b_{n-1,n-1} \end{pmatrix}$$

où la matrice $(b_{i,j})_{1 \leq i,j \leq n-1} \in O_{n-1}(\mathbb{R})$. Il suffit d'appliquer l'hypothèse de récurrence à cette matrice.

Supposons maintenant que $A$ n'a pas de valeur propre réelle. Soit $\lambda := a + ib \in \mathbb{C}$ une valeur propre complexe (non réelle). Soit $Z \in \mathbb{C}^n$ un vecteur propre de $A$ associé. Il existe $X, Y \in \mathbb{R}^n$ tels que $Z = X + iY$. Alors :

$$AX = aX - bY \text{ et } AY = bX + aY$$

Comme $A$ est orthogonale, on a aussi :

$$\langle AX, AX \rangle = \langle X, X \rangle \Rightarrow (a^2 - 1)||X||^2 + b^2||Y||^2 - 2ab\langle X, Y \rangle = 0$$

$$\langle AY, AY \rangle = \langle Y, Y \rangle \Rightarrow (a^2 - 1)||Y||^2 + b^2||X||^2 + 2ab\langle X, Y \rangle = 0$$

$$\langle AX, AY\rangle = \langle X, Y\rangle \Rightarrow (a^2 - b^2 - 1)\langle X, Y\rangle + ab||X||^2 - ab||Y||^2 = 0 \ .$$

On en déduit : $a^2 + b^2 = 1$ et :

$$\langle X, Y\rangle = \frac{b}{2a}(||Y||^2 - ||X||^2) = -\frac{a}{2b}(||Y||^2 - ||X||^2)$$

D'où : si $||Y||^2 \neq ||X||^2$ : $2b^2 = -2a^2$ et $a = b = 0$ absurde donc $||Y||^2 = ||X||^2$ et $\langle X, Y\rangle = 0$.

On peut supposer que $||X|| = ||Y|| = 1$. Soit $R_1 \in O_n(\mathbb{R})$ tel que $R_1X = e_1$. On pose :

$$R_2 := \begin{cases} I_n \text{ si } R_1Y = e_2 \\ R_{\frac{e_2 - R_1Y}{||e_2 - R_1Y||}} \text{ si } R_1Y \neq e_2 \ . \end{cases}$$

Comme $\langle R_1Y, e_1\rangle = \langle R_1Y, R_1X\rangle = \langle Y, X\rangle = 0$, on a $R_2R_1X = e_1$. On a aussi, $R_2R_1Y = e_2$.

Donc $(R_2R_1)^{-1}AR_2R_1$ est une matrice orthogonale de la forme :

$$\begin{pmatrix} U & V \\ 0 & Z \end{pmatrix}$$

où $U \in \mathscr{M}_2(\mathbb{R})$, $Z \in \mathscr{M}_{n-2}(\mathbb{R})$, $V \in \mathscr{M}_{2,n-2}(\mathbb{R})$.

Comme $(R_2R_1)^{-1}AR_2R_1$ est orthogonale, on a :

$$U \in O_2(\mathbb{R})\, ,\ Z \in O_{n-2}(\mathbb{R})\, ,\ {}^t\!VU = 0 \Rightarrow V = 0 \ .$$

Il reste à appliquer l'hypothèse de récurrence à $Z$.

*q.e.d.*

## 9.5 Les quaternions

Rappelons que :

$$\mathbb{C} \simeq \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathscr{M}_2(\mathbb{R}) \right\} \quad a + ib \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ .$$

Sur le même modèle, on peut construire l'algèbre des quaternions à partir de $\mathbb{C}$.

### 9.5.1 Définitions

**Définition 65** *Soit*

$$\mathbb{H} := \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \in \mathscr{M}_2(\mathbb{C}) \right\} .$$

EXEMPLE : Par exemple :

$$1 := I_2,\ I := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} ,\ J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} ,\ K := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \in \mathbb{H} .$$

**Proposition 9.5.1** $\mathbb{H}$ *est une sous-*$\mathbb{R}-$*algèbre de* $\mathscr{M}_2(\mathbb{C})$ i.e. *:* $I_2 \in \mathbb{H}$ *et* $\mathbb{H}$ *est stable par addition, par multiplication par un scalaire réel et par multiplication.*

*Démonstration :* Pour la stabilité par multiplication, on vérifie que :

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \begin{pmatrix} a' & b' \\ -\overline{b'} & \overline{a'} \end{pmatrix} = \begin{pmatrix} aa' - b\overline{b'} & ab' + \overline{a'}b \\ -\overline{ab' + \overline{a'}b} & \overline{aa' - b\overline{b'}} \end{pmatrix} .$$

<u>*q.e.d.*</u>

**Exercice 63** *Vérifier que*

$$\mathbb{H} = \mathbb{R}1 \oplus \mathbb{R}I \oplus \mathbb{R}J \oplus \mathbb{R}K .$$

*Table de mulitplications :*

$$I^2 = J^2 = K^2 = -1$$

$$IJ = -JI = K\ ,\ JK = -KJ = I\ ,\ KI = -IK = J$$

$$IJK = -1$$

(*exo*)

**Remarque :** Si $s \in \mathbb{R}, \vec{v} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \in \mathbb{R}^3$, alors on pose :

$$[s, \vec{v}] := s + v_1 I + v_2 J + v_3 K \in \mathbb{H} .$$

On a alors pour $s, t \in \mathbb{R}$, $\vec{v}$, $\vec{w} \in \mathbb{R}^3$ :

$$[s, \vec{v}][t, \vec{w}] = [st - \vec{v}.\vec{w}, t\vec{v} + s\vec{w} + \vec{v} \wedge \vec{w}] \ .$$

**Définition 66** *On appelle quaternions purs les quaternions de la forme :*

$$xI + yJ + zK \ , \ x, y, z \in \mathbb{R}$$

*et on note* $\mathbb{H}'$ *les sous-espace des quaternions purs.*

On identifiera $\mathbb{R}$ avec $\mathbb{R}I_2 \subseteq \mathbb{H}$.

**Exercice 64** *Pour tout* $q \in \mathbb{H}$ *:*

$$q \in \mathbb{R} \Leftrightarrow q^2 \in \mathbb{R}_+$$

$$q \in \mathbb{H}' \Leftrightarrow q^2 \in \mathbb{R}_-$$

**Remarque :** Pour tout $q = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathbb{H}$, $\text{dét}\, q = |a|^2 + |b|^2$. Donc, $q \neq 0 \Rightarrow q$ inversible dans $\mathscr{M}_2(\mathbb{C})$.

**Proposition 9.5.2** *L'algèbre* $\mathbb{H}$ *est une algèbre à division* i.e. *tout* $q \in \mathbb{H}$ *non nul est inversible dans* $\mathbb{H}$. *De plus, le centre de* $\mathbb{H}$, *c-à-d l'ensemble des* $x \in \mathbb{H}$ *tels que* $xq = qx$ *pour tout* $q \in \mathbb{H}$, *est* $\mathbb{R}$.

*Démonstration :* Soit $0 \neq q = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathbb{H}$. Alors,

$$q^{-1} = \frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \overline{a} & -b \\ \overline{b} & a \end{pmatrix} \in \mathbb{H} \ .$$

Soit $x = a + bI + cJ + dK \in \mathbb{H}$, alors si $x$ est dans le centre de $\mathbb{H}$, on a en particulier :

$$xI = Ix \text{ et } xJ = Jx$$

$$\Rightarrow b = c = d = 0 \ .$$

La réciproque est clair : si $x \in \mathbb{R}$, alors $^\forall q \in \mathbb{H}$, $xq = qx$. *q.e.d.*

**Remarque :** Dans $\mathbb{H}$, l'équation $X^2+1$ a une infinité de solutions, parmi lesquelles : $I, J, K$.

**Exercice 65** *Vérifier que* $Q_8 := \{\pm I_1, \pm I, \pm J, \pm K\}$ *est un sous-groupe de* $\mathbb{H} \setminus \{0\}$.

### 9.5.2 Norme

Pour tout $q \in \mathbb{H}$, on pose :

$$q^* := {}^t\overline{q} \ .$$

*Propriétés :*

$$\forall q_1, q_2 \in \mathbb{H},\ (q_1 q_2)^* = q_2^* q_1^*$$

$$\forall q \in \mathbb{H},\ qq^* = q^* q = \text{dét}\,(q) I_2 \in \mathbb{R}_+ I_2$$

$$\forall a, b, c, d \in \mathbb{R},\ (a + bI + cJ + dK)^* = a - bI - cJ - dK \ .$$

**Définition 67** *On pose pour tout* $q \in \mathbb{H}$, $||q|| := \sqrt{qq^*}$.

**Proposition 9.5.3** *L'application :*

$$\mathbb{H} \times \mathbb{H} \to \mathbb{R}_+ \ (q, q') \mapsto \langle q, q' \rangle := \frac{1}{2}(qq'^* + q' q^*)$$

*est un produit scalaire.*

*Démonstration* : Si $q = a + bI + cJ + dK$, $q' = a' + b'I + c'J + d'K$ avec $a, a', b, b', c, c', d, d'$, alors : $\langle q, q' \rangle = aa' + bb' + cc' + dd'$ ; c'est la formule du produit scalaire standard sur $\mathbb{R}^4$. *q.e.d.*

On remarque :

$$\forall q, q' \in \mathbb{H}, ||qq'|| = ||q|| ||q'||$$

donc :

$$G := S^3 := SU_2 := \{q \in \mathbb{H} \ : \ ||q|| = 1\}$$

est un sous-groupe de $\mathbb{H} \setminus \{0\}$.

Ce groupe joue vis-à-vis des rotations de $SO_3(\mathbb{R})$ le même rôle que le groupe $S^1$ vis-à-vis de $SO_2(\mathbb{R})$.

### 9.5.3 Lien avec les rotations

Pour tout $0 \neq q \in \mathbb{H}$, on pose :

$$s_q : \mathbb{H}' \to \mathbb{H}' \ y \mapsto s_q(y) := qyq^{-1}$$

(vérifier que si $y \in \mathbb{H}'$, $s_q(y) \in \mathbb{H}'$).

Pour tout $0 \neq q \in \mathbb{H}$, on notera $S_q$ la matrice de $s_q$ dans la base $I, J, K$ de $\mathbb{H}'$.

**Remarque :** La base $I, J, K$ de $\mathbb{H}'$ est orthonormale.

**Lemme 9.5.4** *Si $s = s_1 I + s_2 J + s_3 K \in \mathbb{H}'$, avec $s_1, s_2, s_3 \in \mathbb{R}$ et $s_1^2 + s_2^2 + s_3^2 = 1$, alors il existe $g \in S^3$ tel que :*

$$s_g(I) = s \ .$$

*Démonstration :* Il existe $\alpha, \beta \in \mathbb{R}$ tels que :

$$s_1 = \cos\alpha,\ s_2 = \sin\alpha\cos\beta,\ s_3 = \sin\alpha\sin\beta \ .$$

On pose alors :

$$g = \cos\xi I + \sin\xi\cos\eta J + \sin\xi\sin\eta K$$

où $\xi := -\frac{\alpha}{2}$, $\eta = \beta$. On a bien : $s_g(I) = s$. q.e.d.

**Théorème 9.5.5** *Pour tout $q \in S^3$, $S_q \in SO_3(\mathbb{R})$. De plus l'application :*

$$S^3 \to SO_3(\mathbb{R})\ q \mapsto S_q$$

*est un morphisme surjectif de groupes de noyau :* $\pm 1$ i.e. *:*

$$^\forall q, q' \in S^3,\ S_{qq'} = S_q S_{q'}$$

$$S_q = S_{q'} \Leftrightarrow q' = \pm q$$

*et toute rotation $R \in SO_3(\mathbb{R})$ est de la forme $R = S_q$ pour un certain $q \in S^3$.*

*Démonstration : On a bien un morphisme de groupes :*
Soient $q, q' \in S^3$. Alors :

$$^\forall y \in \mathbb{H}',\ s_q s_{q'}(y) = qq'yq'^{-1}q^{-1} = (qq')y(qq')^{-1} = s_{qq'}(y) \ .$$

Donc $s_q s_{q'} = s_{qq'}$ d'où : $S_q S_{q'} = S_{qq'}$.
*On arrive bien dans $O_3(\mathbb{R})$ ...*
De plus :

$$^\forall y \in \mathbb{H}',\ ||s_q(y)|| = ||qyq^{-1}|| = ||q||||y||||q^{-1}|| = ||y||$$

donc $S_q \in O_3(\mathbb{R})$ pour tout $q \in S^3$.
*... plus précisément dans $SO_3(\mathbb{R})$ :*
Nous allons voir que les $S_q$ sont en fait des rotations.
*On commence par un cas particulier :*
*Si $q = a + bI \in S^3$, avec $b \geq 0$,* alors on peut trouver $\theta \in \mathbb{R}$ tel que :

$$a = \cos\frac{\theta}{2} \text{ et } b = \sin\frac{\theta}{2} \ .$$

On vérifie alors que :

$$S_q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} \in SO_3(\mathbb{R}) \ .$$

*Si q est quelconque ...*

Alors : $q = a + p$ où $p \in \mathbb{H}'$. On a alors : $1 = a^2 + ||p||^2$. Si $p = 0$, alors $S_q = I_3 \in SO_3$. Sinon, $\frac{p}{||p||} \in \mathbb{H}'$ et d'après le lemme, il existe $g \in S^3$ tel que :

$$s_g(I) = gIg^{-1} = \frac{p}{||p||} \ .$$

On a alors :

$$s_g(a + ||p||I) = q$$

(*exo*) .

Soit $r := a + ||p||I$. On a donc : $grg^{-1} = q$ d'où :

$$S_q = S_g S_r S_g^{-1}$$

or $S_r \in SO_3(\mathbb{R})$ d'après la première partie de la démonstration donc $S_q \in SO_3(\mathbb{R})$ (car de déterminant 1).

*Il reste à montrer la surjectivité* :

Soit $R \in SO_3(\mathbb{R})$. Il existe un vecteur propre $v := \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \in \mathbb{R}^3$ de poids 1 de $R$.D'après le lemme, il existe $g \in S^3$ tel que : $s_g(I) = v_1 I + v_2 J + v_3 K$. Mais alors :

$$S_g^{-1} R S_g \left( \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \ .$$

Donc, comme $S_g^{-1} R S_g \in SO_3(\mathbb{R})$, on a :

$$S_g^{-1} R S_g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$$

pour un certain $\theta \in \mathbb{R}$. Donc si on pose :

$$r := \cos\frac{\theta}{2} + \sin\frac{\theta}{2} I$$

on a :

$$S_g^{-1} R S_g = S_r \Leftrightarrow R = S_g S_r S_g^{-1}$$
$$\Leftrightarrow R = S_{grg^{-1}}$$

d'où la surjectivité.

*Pour finir le noyau est* $\{\pm 1\}$ *:*

Si $S_q = I_3$ alors :

$$^{\forall} y \in \mathbb{H}',\, s_q(y) = y$$
$$\Leftrightarrow {}^{\forall} y \in \mathbb{H}',\, qyq^{-1} = y \Leftrightarrow qy = yq$$
$$\Leftrightarrow {}^{\forall} y \in \mathbb{H},\, qy = yq$$
$$\Leftrightarrow q \in \mathbb{R}\ .$$

Si $q \in S^3$, alors $||q|| = |q| = 1 \Rightarrow q = \pm 1$.

*q.e.d.*

**Exercice 66** *Soit* $q \in S^3$*. Si* $q = \pm 1$*, alors* $S_q = I_3$*. Sinon,* $q = a + p$ *avec* $a \in \mathbb{R}$*,* $0 \neq p \in \mathbb{H}'$ *et* $a^2 + ||p||^2 = 1$*. Mais alors il existe* $\theta \in \mathbb{R}$ *tel que :*

$$a = \cos\frac{\theta}{2} \text{ et } ||p|| = \sin\frac{\theta}{2}\ .$$

*Posons aussi* $\vec{p} := \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}$ *si* $p = p_1 I + p_2 J + p_3 K$*. Avec ces notations,* $S_q$ *est la rotation d'axe* $\mathbb{R}\vec{p}$ *et d'angle* $\theta$*.*

# Chapitre 10

# Invariants de similitude

## 10.1 Matrices à coefficients polynomiaux

**Lemme 10.1.1** *Soit $A \in \mathscr{M}_n(\mathbb{K}[X])$. La matrice $A$ est inversible dans $\mathscr{M}_n(\mathbb{K}[X])$ si et seulement si* $\text{dét}\, A$ *est une constante non nulle. Autrement dit :*

$$\mathrm{GL}_n(\mathbb{K}[X]) = \{A \in \mathscr{M}_n(\mathbb{K}[X]) \ : \ \text{dét}\, A \in \mathbb{K}^*\} \ .$$

*Démonstration :* Si $AB = I_n$ pour une matrice $B \in \mathscr{M}_n(\mathbb{K}[X])$, alors :

$$\text{dét}\, A \text{dét}\, B = 1$$

donc $\text{dét}\, A$ est un polynôme inversible. Donc $\text{dét}\, A \in \mathbb{K} \setminus \{0\}$. Réciproquement, si $\text{dét}\, A \in \mathbb{K} \setminus \{0\}$, alors :

$$A^{-1} = \frac{1}{\text{dét}\, A} {}^t\widetilde{(A)} \in \mathscr{M}_n(\mathbb{K}[X]) \ .$$

*q.e.d.*

**Définition 68** *On notera pour toute matrice non nulle $A \in \mathscr{M}_n(\mathbb{K}[X])$*

$$d_1(A) := \text{ le pgcd unitaire des coefficients de } A$$

*c'est le polynôme unitaire de degré maximal qui divise tous les coefficients de $A$.*

**Proposition 10.1.2** *Si $P, Q \in \mathscr{M}_n(\mathbb{K}[X])$ sont des matrices inversibles (c-à-d dont le déterminant est une constante non nulle), alors $d_1(PAQ) = d_1(A)$.*

*Démonstration* : Notons $c_{i,j}$ les coefficients de $PAQ$. Alors :

$$\forall i, j \,,\; c_{i,j} = \sum_{k,l=1}^{n} P_{i,k} A_{k,l} Q_{l,j}$$

donc $d_1(A)$ divise $c_{i,j}$ pour tous $i, j$. Donc $d_1(A)$ divise $d_1(PAQ)$. De même $d_1(PAQ)$ divise $d_1(A) = d_1(P^{-1}(PAQ)Q^{-1})$. Ainsi, $d_1(A) = d_1(PAQ)$. q.e.d.

### 10.1.1 Matrices élémentaires

Ce sont les matrices de l'une des formes suivantes :

$T_{i,j}(\lambda)$ « la matrice $I_n$ à laquelle on a ajouté un polynôme $\lambda \in \mathbb{K}[X]$ en position $i, j$ »

$$\begin{pmatrix} 1 & \dots & \lambda(X) & \\ & \ddots & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

— $\Sigma_i$ « la matrice obtenue à partir de $I_n$ en permutant les colonnes $i$ et $i+1$ » :

$$\Sigma_i := \begin{pmatrix} 1 & & & & & \\ & \overset{i-1 \text{ fois}}{\ddots} & & & & \\ & & 1 & & & \\ & & & 0 & 1 & & \\ & & & 1 & 0 & & \\ & & & & & 1 & \\ & & & & & & \overset{i-1 \text{ fois}}{\ddots} \\ & & & & & & & 1 \end{pmatrix}$$

— $D_i(\alpha)$ « la matrice obtenue à partir de $I_n$ en remplaçant le $i$ème coefficient diagonal par $\alpha \in \mathbb{K}^*$ :

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & \alpha & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} .$$

**Remarque :** Ces matrices sont toutes inversibles dans $\mathscr{M}_n(\mathbb{K}[X])$.

## 10.2 Réduction des matrices à coefficients polynomiaux

**Définition 69** *Soient $A, B \in \mathscr{M}_n(\mathbb{K}[X])$. On dira que $A$ est équivalente à $B$, notation : $A \sim B$ s'il existe $P, Q \in \mathrm{GL}_n(\mathbb{K}[X])$ telles que : $A = PBQ$.*

**Exercice 67** *C'est une relation d'équivalence* i.e. *:*

$$^\forall A, B, C \in \mathscr{M}_n(\mathbb{K}[X]),\ A \sim A\ ;$$

$$A \sim B \Rightarrow B \sim A\ ;$$

$$A \sim B \sim C \Rightarrow A \sim C\ .$$

**Lemme 10.2.1** *Soit $A \in \mathscr{M}_n(\mathbb{K}[X])$ une matrice non nulle. Alors, $A$ est équivalente à une matrice de la forme :*

$$\begin{pmatrix} d_1(A) & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}$$

*pour une certaine matrice $A' \in \mathscr{M}_{n-1}(\mathbb{K}[X])$.*

*Démonstration :* On utilise la multiplication à gauche et à droite par des matrices élémentaires. Dans le tableau suivant, on rappelle l'effet de la multiplication d'une matrice $A$ par les matrices élémentaires :

| Matrices élémentaires $E$ | effet de la multiplication à gauche $EA$ | effet de la multiplication à droite $AE$ |
|---|---|---|
| $T_{i,j}(\lambda)$ | « ajoute $\lambda\times$ la ligne $i$ à la ligne j » | « ajoute $\lambda\times$ la colonne $i$ à la colonne $j$ » |
| $D_i(\alpha)$ | « multiplie la ligne $i$ par $\alpha$ » | « multiplie la colonne $i$ par $\alpha$ » |
| $\Sigma_i$ | « échange les lignes $i$ et $i+1$ » | « échange les colonnes $i$ et $i+1$ » |

Soit $d$ le degré minimal d'un coefficient non nul $b_{i,j}$ d'une matrice $B$ équivalente à $A$. Quitte à permuter des lignes ou des colonnes de $B$, on peut

supposer que $b_{1,1}$ est de degré $d$. Soit $2 \leq j \leq n$, la division euclidienne de $b_{1,j}$ par $b_{1,1}$ donne :

$$b_{1,j} = qb_{1,1} + r_{1,j}$$

où $\deg r_{1,j} < \deg b_{1,1}$. Donc en retranchant $q\times$ la colonne 1 à la colonne $j$ de $B$ on obtient une matrice équivalente à $B$ donc à $A$ dont la première ligne est de la forme :

$$b_{1,1} ... r_{1,j} ...$$

Si $r_{1,j} \neq 0$, on a contredit la minimalité de $d$. Donc $r_{1,j} = 0$ et $b_{1,1}$ divise $b_{1,j}$. En raisonnant comme cela avec tous les colonnes $2 \leq j \leq n$ et de même avec toutes les lignes $2 \leq i \leq n$, on s'aperçoit que l'on peut supposer que les coefficients $b_{1,j}$ et $b_{i,1}$ sont nuls si $2 \leq i, j \leq n$. Soit $b_{i,j}$ un coefficient de $B$ avec $i, j \geq 2$. En ajoutant la ligne $i$ à la ligne 1, on trouve une matrice équivalente à $A$ dont la première ligne comprend les termes :

$$b_{1,1} ... b_{i,j} ...$$

On a alors vu que $b_{1,1}$ divise $b_{i,j}$.

On a donc montré que $A$ est équivalente à une matrice $B$ de la forme :

$$\begin{pmatrix} b_{1,1} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}$$

où $b_{1,1}$ divise tous les coefficients de la matrice $A'$ et où l'on peut supposer que $b_{1,1}$ est unitaire (quitte à multiplier la ligne 1 par un coefficient constant non nul) . Mais alors $d_1(B) = b_{1,1}$. Et comme $A$ est équivalente à $B$, $d_1(A) = b_{1,1}$.

*q.e.d.*

Exemple :

$$\begin{pmatrix} X & -1 \\ 0 & X \end{pmatrix} \underset{\sim}{C_1 \leftrightarrow C_2} \begin{pmatrix} -1 & X \\ X & 0 \end{pmatrix} \underset{\sim}{-C_1} \begin{pmatrix} 1 & X \\ -X & 0 \end{pmatrix}$$

$$\underset{\sim}{L_2 \leftarrow L_2 + XL_1} \begin{pmatrix} 1 & X \\ 0 & X^2 \end{pmatrix} \underset{\sim}{C_2 \leftarrow C_2 - XC_1} \begin{pmatrix} 1 & 0 \\ 0 & X^2 \end{pmatrix} .$$

**Théorème 10.2.2** *Soit $A \in \mathscr{M}_n(\mathbb{K}[X])$. Alors, il existe $r \geq 0$ et une suite $P_1, ..., P_r$ de polynômes unitaires dans $\mathbb{K}[X]$ tels que :*

$$i) \;\; P_1 | P_2 | ... | P_r$$

$$ii) \;\; A \sim \begin{pmatrix} P_1 & & & & & \\ & \ddots & & & & \\ & & P_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

*(« | » signifie divise). De plus, si $s \geq 0$ et une suite $Q_1, ..., Q_s$ de polynômes unitaires vérifient aussi i)etii), alors : $s = r$ et $Q_i = P_i$ pour tout $1 \leq i \leq r$.*

*Démonstration :* Pour l'existence des $P_1, ..., P_r$, il suffit de raisonner par récurrence sur $n$, la taille de la matrice $A$, et d'utiliser le lemme 10.2.1.

Pour l'unicité, on peut aussi raisonner par récurrence sur $n$.

Si on a :

$$\begin{pmatrix} P_1 & & & & & \\ & \ddots & & & & \\ & & P_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} \sim A \sim \begin{pmatrix} Q_1 & & & & & \\ & \ddots & & & & \\ & & Q_s & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

et $P_1 | ... | P_r$, $Q_1 | ... | Q_s$ alors on peut supposer $A \neq 0$ et on a forcément $P_1 = Q_1 = d_1(A)$. Mais alors :

$$\begin{pmatrix} P_1 & & & & & \\ & \ddots & & & & \\ & & P_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} \sim \begin{pmatrix} P_1 & & & & & \\ & \ddots & & & & \\ & & Q_s & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

entraîne

$$\begin{pmatrix} P_2 & & & & & \\ & \ddots & & & & \\ & & P_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} \sim \begin{pmatrix} Q_2 & & & & & \\ & \ddots & & & & \\ & & Q_s & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

(*exo*) *q.e.d.*

**Remarque :** Si dét $A \neq 0$, alors $r = n$ et dét $A = P_1 ... P_n$.

**Définition 70** *Les $P_i$ différents de 1 sont appelés les diviseurs élémentaires de A. Si $A \in \mathscr{M}_n(\mathbb{K})$, les diviseurs élémentaires de $XI_n - A$ sont appelés les invariants de similitude de A.*

**Exercice 68** *Si $A, B \in \mathscr{M}_n(\mathbb{K})$ sont semblables, alors A et B ont les mêmes invariants de similitude. Pour la réciproque, cf. la section suivante.*

## 10.3 Invariants de similitude

*Quels sont les invariants de similitude d'une matrice compagnon ?*

**Lemme 10.3.1** *Soient $P(X) := X^n + a_1 X^{n-1} + ... + a_n \in \mathbb{K}[X]$ et*

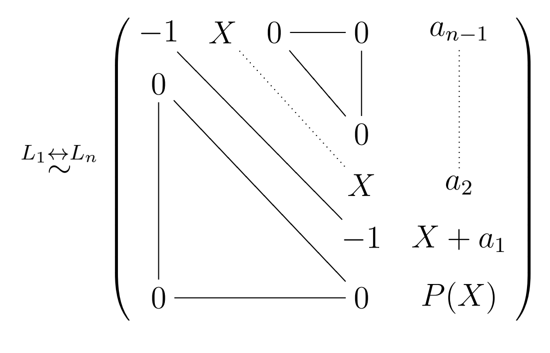
$$C_P := \begin{pmatrix} 0 & \cdots & 0 & -c_n \\ 1 & \ddots & \vdots & \vdots \\ 0 & \ddots & \vdots & \vdots \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots\ 0 & 1 & -c_1 \end{pmatrix} \in \mathscr{M}_n(\mathbb{K})$$

*la matrice compagnon associée. Alors la matrice $C_P$ a un seul invariant de similitude : le polynôme $P(X)$.*

*Démonstration :*

$$XI_n - C_P := \begin{pmatrix} X & 0 & \cdots & 0 & a_n \\ -1 & \ddots & \ddots & \vdots & \vdots \\ 0 & \ddots & \ddots & 0 & \\ \vdots & \ddots & \ddots & X & \\ 0 & \cdots & 0 & -1 & X + a_1 \end{pmatrix}$$

$$\underset{L_1 \leftarrow L_1 + XL_2 + \ldots + X^{n-1}L_n}{\sim} \begin{pmatrix} 0 & 0 & \cdots & 0 & P(X) \\ -1 & X & \ddots & \vdots & \vdots \\ 0 & \ddots & \ddots & 0 & \\ \vdots & \ddots & \ddots & X & \\ 0 & \cdots & 0 & -1 & X + a_1 \end{pmatrix}$$



$$\sim \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 & \\ & & & P(X) \end{pmatrix}$$

<u>*q.e.d.*</u>

**Lemme 10.3.2** *Soient $A, B \in \mathscr{M}_n(\mathbb{K})$. alors :*

$$XI_n - A \sim XI_n - B \Leftrightarrow A \textit{ est semblable à } B.$$

*Démonstration :* Démontrons le sens difficile : $\Rightarrow$ : on suppose qu'il existe $P, Q \in \mathrm{GL}_n(\mathbb{K}[X])$ telles que :

$$XI_n - A = P(XI_n - B)Q \ .$$

*Il existe deux matrices* $P_0, P_1 \in \mathscr{M}_n(\mathbb{K})$ *telles que* $P = (XI_n - A)P_1 + P_0$.

En effet, comme $XI_n - A$ et $A$ commutent, on a pour tout $k \geq 1$ :

$$X^k I_n = ((XI_n - A) + A)^k = (XI_n - A)R_k + A^k$$

pour une certaine matrice $R_k \in \mathscr{M}_n(\mathbb{K}[X])$ † . Or, $P = X^m C_m + ... + C_0$ pour certaines matrices $C_0, ..., C_m \in \mathscr{M}_n(\mathbb{K})$ (on a simplement décomposé les coefficients en somme de monômes et regroupé les monômes par degrés). Donc :

$$P = (XI_n - A)\underbrace{(R_m + ... + R_1)}_{=:P_1} + \underbrace{(A^m C_m + ... + C_0)}_{=:P_0} \ .$$

De même, il existe $Q_0, Q_1 \in \mathscr{M}_n(\mathbb{K}[X])$ telles que $Q = Q_1(XI_n - A) + Q_0$.

Mais alors :

$$XI_n - A = ((XI_n - A)P_1 + P_0)(XI_n - B)(Q_1(XI_n - A) + Q_0)$$

$$= P_0(XI_n - B)Q_0 + (XI_n - A)P_1(XI_n - B)Q_1(XI_n - A)$$

$$+ P_0(XI_n - B)Q_1(XI_n - A) + (XI_n - A)P_1(XI_n - B)Q_0 \ .$$

Or :

$$P_0(XI_n - B)Q_1(XI_n - A) = (P - (XI_n - A)P_1)(XI_n - B)Q_1(XI_n - A)$$

$$= (XI_n - A)\left( Q^{-1}Q_1 - P_1(XI_n - B)Q_1 \right)(XI_n - A)$$

car $P(XI_n - B) = (XI_n - A)Q^{-1}$.

De même :

$$(XI_n - A)P_1(XI_n - B)Q_0 = (XI_n - A)\left( P_1 P^{-1} - P_1(XI_n - B)Q_1 \right)(XI_n - A).$$

On a donc montré que :

$$XI_n - A = P_0(XI_n - B)Q_0 + (XI_n - A)S(XI_n - A)$$

où :

$$S := Q^{-1}Q_1 - P_1(XI_n - B)Q_1 + P_1 P^{-1} \in \mathscr{M}_n(\mathbb{K}[X]) \ .$$

Finalement, on a obtenu :

$$XI_n - A - P_0(XI_n - B)Q_0 = (XI_n - A)S(XI_n - A) \ .$$

†. il suffit de prendre $R_k = \sum_{j=0}^{k-1} \binom{k}{j} (XI_n - A)^{k-j-1} A^j$.

Si $S \neq 0$, le terme de droite est de degré au moins 2 alors que le terme de gauche est toujours de degré $\leq 1$ : *contradiction !*

Donc $S = 0$ et :

$$XI_n - A = P_0(XI_n - B)Q_0$$

avec $P_0, Q_0 \in \mathscr{M}_n(\mathbb{K})$. Enfin, on conclut :

$$XI_n - A = P_0(XI_n - B)Q_0 \Leftrightarrow XI_n - A = XP_0Q_0 - P_0BQ_0$$

$$\Leftrightarrow P_0Q_0 = I_n \text{ et } A = P_0BQ_0$$

$$\Rightarrow P_0 \text{ inversible et } A = P_0BP_0^{-1} \ .$$

*q.e.d.*

Voici le théorème principal du chapitre (et même du cours) :

**Théorème 10.3.3** *Soit* $A \in \mathscr{M}_n(\mathbb{K})$. *Il existe* $1 \leq r \leq n$ *et* $P_1, ..., P_r \in \mathbb{K}[X]$ *des polynômes unitaires tels que :*

$$i) \ \ P_1|...|P_r \ ;$$

$$ii) \ \ XI_n - A \sim \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & P_1 & & \\ & & & & \ddots & \\ & & & & & P_r \end{pmatrix} .$$

*De plus, A est semblable à la matrice diagonale par blocs :*

$$\begin{pmatrix} C_{P_1} & & \\ & \ddots & \\ & & C_{P_r} \end{pmatrix}$$

*où les* $C_{P_i}$ *sont les matrices compagnons associées aux polynômes* $P_i$. *En particulier :*

$$\chi_A(X) = P_1...P_r \text{ et } P_r \textit{ est le polynôme minimal de } A.$$

**Corollaire 10.3.3.1** *Si* $A, B \in \mathscr{M}_n(\mathbb{K})$ *ont les mêmes invariants de similitude alors A et B sont semblables.*

*Démonstration :* $A$ et $B$ sont semblables à la même matrice diagonale par blocs « compagnons » d'après le théorème. *q.e.d.*

*Démonstration du théorème principal :* Soient $P_1, ..., P_r$ les invariants de similitude de $A$. Alors $i)$ et $ii)$ sont vérifiées.En particulier :

$$XI_n - A = P \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & P_1 & & \\ & & & & \ddots & \\ & & & & & P_r \end{pmatrix} Q$$

pour certaines matrices $P, Q \in \mathrm{GL}_n(\mathbb{K}[X])$. En prenant le déterminant, on trouve :

$$\chi_A(X) = \text{dét}\, P(P_1...P_r)\text{dét}\, Q$$

$$\Rightarrow \chi_A(X) = cP_1...P_r$$

où $c := \text{dét}\, P\text{dét}\, Q \in \mathbb{K}^*$. Comme $\chi_A(X)$ et $P_1...P_r$ sont unitaires, $c = 1$.

En particulier, $\deg \chi_A(X) = n = \deg P_1 + ... + \deg P_r$. Donc dans la matrice $\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & P_1 & & \\ & & & & \ddots & \\ & & & & & P_r \end{pmatrix}$, le nombre de « 1 » sur la diagonal est :

$$n - r = (\deg P_1 - 1) + ... + (\deg P_r - 1) \ .$$

On en déduit que :

$$\left(\begin{array}{c|c|c} C_{P_1} & & \\ \hline & \ddots & \\ \hline & & C_{P_r} \end{array}\right) \in \mathscr{M}_n(\mathbb{K})$$

et que :

$$\left(\begin{array}{c|c|c} C_{P_1} & & \\ \hline & \ddots & \\ \hline & & C_{P_r} \end{array}\right) \sim \left(\begin{array}{c|c|c} \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & P_1 \end{pmatrix} & & \\ \hline & \ddots & \\ \hline & & \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & P_r \end{pmatrix} \end{array}\right)$$

$$\sim \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & P_1 & & \\ & & & & \ddots & \\ & & & & & P_r \end{pmatrix} \sim XI_n - A \ .$$

On applique alors le lemme 10.3.2 aux matrices $A$ et $\left(\begin{array}{c|c|c} C_{P_1} & & \\ \hline & \ddots & \\ \hline & & C_{P_r} \end{array}\right)$.

Il reste à montrer que $P_r$ est le polynôme minimal de $A$. Il suffit de vérifier que $P_r$ est le polynôme minimal de $\mathscr{C} := \left(\begin{array}{c|c|c} C_{P_1} & & \\ \hline & \ddots & \\ \hline & & C_{P_r} \end{array}\right)$. Or, un polynôme $p(X)$ annule $\mathscr{C}$ si et seulement si $p(C_{P_1}) = ... = p(C_{P_r}) = 0$ *i.e.* $P_i | p(X)$ pour tout $i$ (car $C_{P_i}$ a pour polynôme minimal $P_i$). Donc :

$$p(\mathscr{C}) = 0 \Leftrightarrow P_r | p(X) \ .$$

Ainsi, $\mathscr{C}$, et donc $A$, ont pour polynôme minimal $P_r$. <u>*q.e.d.*</u>

## 10.4 Endomorphismes cycliques

Soit $E$ un $\mathbb{K}-$espace vectoriel de dimension finie.

Soit $u$ un endomorphisme de $E$.

Les facteurs invariants $P_1, ..., P_r$ de la matrice de $u$ dans une base de $E$ ne dépendent pas de la base choisie ; on les appellera les facteurs invariants de $u$.

Pour tout $x$ de $E$, on note :

$$E_x := \langle x, u(x), ..., u^k(x), ... \rangle \ .$$

*Remarque :* $E_x = \{P(u)(x) \ : \ P(X) \in \mathbb{K}[X]\}$.

Le sous-espace $E_x$ est stable par $u$. De plus si $P(X) \in \mathbb{K}[X]$ est un polynôme annulateur de $u$ (par exemple le polynôme minimal de $u$), alors $E_x$ est engendré par les vecteurs $x, ..., u^{d-1}(x)$ où $d$ est le degré de $P(X)$ (*exo*) .

**Définition 71** *On dit que $u$ est un endomorphisme cyclique s'il existe $x \in E$ tel que $E_x = E$.*

**Proposition 10.4.1** *Soit $u$ un endomorphisme de $E$ de polynôme minimal $m_u(X)$.*

*L'endomorphisme $u$ est cyclique si et seulement si $\deg m_u = \dim E$ (i.e. $m_u(X) = \chi_u(X)$ le polynôme caractéristique de $u$.*

*Démonstration :* Soit $d := \deg m_u(X)$. Soit $n := \dim E$. Si $E_x = E$, alors il existe $k \leq d$ tel que $x, ..., u^{k-1}(x)$ forment une base de $E_x$. On a donc :

$$k = \dim E_x = \dim E = n \leq d$$

Donc $\deg \chi_u(X) \leq \deg m_u(X)$. Or, $m_u(X)$ divise $\chi_u(X)$ et les deux sont unitaires donc : $\chi_u = m_u$.

Pour la réciproque on utilise les facteurs invariants $P_1, ..., P_r$ de $u$. On a $P_1|...|P_r$, $P_1...P_r = \chi_u(X)$ et $P_r = m_u(X)$. Si $m_u(X) = \chi_u(X)$, alors $r = 1$ et il existe une base $e_1, ..., e_n$ de $E$ où la matrice de $u$ est une matrice compagnon : $C_{P_1}$.

On a alors :

$$u(e_i) = e_{i+1}$$

si $1 \leq i \leq n$. Donc :

$$E = \langle e_1, ..., e_n \rangle = \langle e_1, ..., u^{n-1}(e_1) \rangle$$

$$= E_{e_1}$$

et $u$ est cyclique.

*q.e.d.*

*Remarque :* si $u$ est cyclique et si $E = E_x$, alors pour tout $P \in \mathbb{K}[X]$, on a :

$$P(u)(x) = 0 \Leftrightarrow P(u) = 0 \Leftrightarrow m_u(X)|P(X) \ .$$

En effet, si $P(u)(x) = 0$, alors $P(u)(u^k(x)) = u^k(P(u)(x)) = 0$ pour tout $k$, donc $P(u)$ est nul sur $E_x = E$.

En particulier, si $E_x = E$, alors : $x, u(x), ..., u^{n-1}(x)$ est une base de $E$.

Voici une version du théorème 10.3.3 pour les endomorphismes :

**Théorème 10.4.2** *Si $u$ est un endomorphisme de $E$, alors il existe une suite de sous-espaces stables de $E$ : $E_1, ..., E_r$ tels que :*

*i) $E = E_1 \oplus ... \oplus E_r$ ;*

*ii) pour tout $1 \le i \le r$, la restriction $u_i := u|_{E_i}$ est un endomorphisme cyclique ;*

*iii) si pour tout $i$, $P_i$ est le polynôme minimal de $u_i$, alors $P_1|...|P_r$.*

*De plus la suite $P_1, ..., P_r$ ne dépend pas de la décomposition choisie. Ce soont les facteurs invariants de $u$.*

*Remarque :* il existe une base $e_1, ..., e_n$ de $E$ où la matrice de $u$ est de la forme :

$$\begin{pmatrix} C_{P_1} & & \\ & \ddots & \\ & & C_{P_r} \end{pmatrix}$$

c'est la réduction de Frobenius.

**Théorème 10.4.3 (Frobenius)** *Soit $u$ un endomorphisme de $E$. Notons $P_1, ..., P_r$ ses facteurs invariants. On note :*

$$\mathscr{C}(u) := \{v \in \mathscr{L}(E) \ : \ uv = vu\}$$

*l'espace des endomorphismes qui commutent à $u$. Alors :*

$$\dim \mathscr{C}(u) = (2r-1)d_1 + (2r-3)d_2 + ... + d_r$$

*où $d_i := \deg P_i$ pour tout $i$.*

*Démonstration :* Soit $E = E_1 \oplus ... \oplus E_r$ une décomposition comme dans le théorème 10.4.2. On n ote $u_i := u|_{E_i}$. Pour tout $x \in E$ on pose $f_j(x$ la composante de $f(x)$ dans $E_j$ :

$$f(x) = f_1(x) + ... + f_r(x)$$

avec $f_1j(x) \in E_j$ pour tout $j$. Alors $f_j : E \to E_j$, $x \mapsto f_j(x)$ est linéaire. Pour tous $1 \leq i, j \leq r$, on pose :

$$f_{i,j} := f_j|_{E_i} : E_i \to E_j \ .$$

L'application :

$$\mathscr{L}(E) \to \oplus_{1\leq i,j\leq r}\mathscr{L}(E_i, E_j)$$

est un isomorphisme (*exo*) .

Pour tous $1 \leq i, j \leq r$, on pose

$$\mathscr{C}_{i,j} := \{F \in \mathscr{L}(E_i, E_j) \ : \ u_j F = F u_i\} \ .$$

On a :

$$f \in \mathscr{C}(u) \Leftrightarrow fu = uf \Leftrightarrow {}^\forall 1 \leq i \leq r,\ {}^\forall x \in E_i,\ fu(x)uf(x)$$

$${}^\forall 1 \leq i \leq r,\ {}^\forall x \in E_i,\ f_1u(x) + ... + f_ru(x) = uf_1(x) + ... + uf_r(x)$$

$$\Leftrightarrow {}^\forall 1 \leq i \leq r,\ {}^\forall x \in E_i,\ {}^\forall 1 \leq j \leq r,\ f_ju(x) = uf_j(x)$$

$${}^\forall 1 \leq i, j \leq r,\ f_ju_i = u_jf_j|_{E_i}$$

$${}^\forall 1 \leq i, j \leq r,\ f_{i,j}u_i = u_jf_{i,j} \ .$$

Donc $\mathscr{C}(u) \simeq \oplus_{1\leq i,j\leq r}\mathscr{C}_{i,j}$ et :

$$\dim \mathscr{C}(u) = \sum_{1\leq i,j\leq r} \dim \mathscr{C}_{i,j} \ .$$

Calculons $\dim \mathscr{C}_{i,j}$ : soit $x \in E_i$ tel que :

$$E_i = \langle x, ..., u_i^{d_i-1}(x)\rangle = \langle x, ..., u^{d_i-1}(x)\rangle$$

(en particulier, $x, ..., u^{d_i-1}(x)$ est une base de $E_i$).

Soit $\Phi : \mathscr{C}_{i,j} \to E_j$, $F \mapsto F(x)$.

Alors $\Phi$ est injective :

en effet, si $F \in \mathscr{C}_{i,j}$ et si $\Phi(F) = 0$, alors $F(x) = 0$ et pour tout $k \geq 0$, on a :

$$Fu_i^k(x) = u_j^kF(x) = 0$$

donc $F$ est nul sur $E_i$ *i.e.* $F = 0$.

On a $\mathrm{Im}\,\Phi = \ker P_i(u_j) \subseteq E_j$.

En effet, si $F \in \mathscr{C}_{i,j}$, alors :

$$P_i(u_j)(F(x)) = (P_i(u_j)F)(x)$$

$$= (FP_i(u_i))(x)$$
$$= 0 \ .$$

Donc $F(x) \in \ker P_i(u_j)$ pour tout $F \in \mathscr{C}_{i,j}$. ainsi : $\mathrm{Im}\,\Phi \subseteq \ker P_i(u_j)$.

Pour l'inclusion réciproque, soit $y \in \ker P_i(u_j)$. On pose alors :

$$F(Q(u_i)(x)) := Q(u_j)(y)$$

pour tout polynôme $Q$. L'application $F : E_i \to E_j$ est bien définie en effet : si $Q_1, Q_2 \in \mathbb{K}[X]$ sont des polynômes tels que $Q_1(u_i)(x) = Q_2(u_i)(x)$, alors

$$(Q_1 - Q_2)(u_i)(x) = 0 \Rightarrow P_i | Q_1 - Q_2$$

(car $P_i$ est le polynôme minimal de $u_i$)

$$\Rightarrow (Q_1 - Q_2)(u_j)(y) = 0$$

(car $y \in \ker(P_i(u_j))$)

$$\Rightarrow Q_1(u_j)(y) = Q_2(u_j)(y) \ .$$

L'application est linéaire et on a : $Fu_i(x) = u_j(y)$ et $F(x) = y$ donc :

$$Fu_i(x) = u_j F(x)$$

$$\Rightarrow Fu_i = u_j F$$

sur $E_i$.

Ainsi, $F \in \mathscr{C}_{i,j}$ et $\Phi(F) = F(x) = y$.

On a donc $\dim \mathscr{C}_{i,j} = \dim \ker P_i(u_j)$.

Nous allons montrer que :

$$\dim \ker P_i(u_j) = \begin{cases} d_i \text{ si } i \leq j \\ d_j \text{ si } i \geq j \end{cases} \ .$$

Si $i \geq j$, alors $P_j | P_i$ donc $P_i(u_j) = 0$ et $\ker P_i(u_j) = \ker 0 = E_j$. Donc $\dim \ker P_i(u_j) = \dim E_j = d_j$.

Si $i \leq j$, alors $P_i | P_j$. Soit $Q \in \mathbb{K}[X]$ tel que $P_i Q = P_j$.

Soit $S \in \mathbb{K}[X]$. On a : $S(u_j)(x) \in E_j$ et :

$$S(u_j)(x) \in \ker P_i(u_j) \Leftrightarrow P_i(u_j)S(u_j)(x) = 0$$

$$\Leftrightarrow P_j | P_i S$$

$$\Leftrightarrow P_i Q | P_i S$$

$$\Leftrightarrow Q|S \ .$$

Donc :

$$\ker P_i(u_j) = \{S(u_j)(x) \ : \ Q|S\}$$
$$= \{(QS_1)(u_j)(x) \ : \ S_1 \in \mathbb{K}[X]\}$$
$$= \left\langle Q(u_j)(u_j^k(x)) \ : \ k \geq 0 \right\rangle$$
$$= \left\langle Q(u_j)(u_j^k(x)) \ : \ 0 \leq k \leq d_i - 1 \right\rangle$$

(*exo*) .

Or les vecteurs $Q(u_j)(u_j^k(x)) \ : \ 0 \leq k \leq d_i - 1$ sont indépendants donc $\dim \ker P_i(u_j) = d_i$.

En conclusion, on a :

$$\dim \mathscr{C}(u) = \sum_{1 \leq i,j \leq r} \dim \mathscr{C}_{i,j}$$
$$= \sum_{1 \leq i < j \leq r} d_i + \sum_{1 \leq j < i \leq r} d_j + \sum_{1 \leq i \leq r} d_i$$
$$= 2 \sum_{1 \leq i < j \leq r} d_i + \sum_{1 \leq i \leq r} d_i$$
$$= 2 \sum_{1 \leq i \leq r} (r-i) d_i + \sum_{1 \leq i \leq r} d_i$$
$$= \sum_{1 \leq i \leq r} (2r - 2i + 1) d_i \ .$$

*q.e.d.*

*Remarques :*

— si $u = \lambda \mathrm{Id}_E$, alors $r = n$ et les facteurs invariants de $u$ sont $P_1 = ... = P_r = (X - \lambda)$ et on retrouve que :

$$\dim \mathscr{C}(u) = \sum_{1 \leq i \leq r} (2n - 2i - 1)$$
$$= 2n - 1 + 2n - 3 + ... + 1$$
$$= n^2 = \dim \mathscr{L}(E) \ .$$

D'où $\mathscr{C}(u) = \mathscr{L}(E)$.

— si $u$ est cyclique, alors : $r = 1$ et $P_1 = \chi_u(X)$ donc :

$$\dim \mathscr{C}(u) = n \ .$$

On en déduit dans ce cas que :

$$\mathscr{C}(u) = \mathbb{K}[u]$$

$$= \{P(u) \;:\; P \in \mathbb{K}[X]\}$$

$$= \langle \mathrm{Id}_E, u, ..., u^{n-1} \rangle \;.$$

# Index